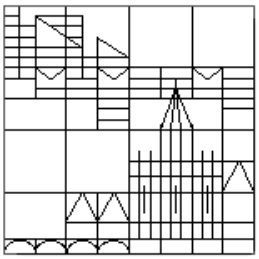


Universität Konstanz

Informationswissenschaft

Eine Software-Plattform
für
elektronische Zahlungssysteme im Internet

unter Berücksichtigung der
speziellen Anforderungen einer Mall.

Diplomarbeit

vorgelegt von

Annette Wolf

Mai 1998

Gutachter:

Prof. Dr. Rainer Kuhlen

Prof. Dr. Harald Reiterer

Fachliche Betreuung:

Wolfgang Semar

Inhaltsangabe

Eine Vielzahl der Entwicklungen im Internet sind transaktionsorientiert, geprägt durch den kommerziellen Austausch von und Handel mit Waren und Dienstleistungen. Aktuell herrscht ein wahrer Wildwuchs an Systemen und Anwendungen für Teilbereiche des *Electronic Commerce* und speziell für den Bereich elektronische Zahlungssysteme, der als kritischer Erfolgsfaktor für die Verbreitung des E-Commerce im Internet eingestuft werden und die Gegenstand dieser Arbeit sind.

Vor dem Hintergrund dieser fragmentarischen Situation, wird auf die speziellen Interessenschwerpunkte einer Mall eingegangen und die Motive für den Einsatz von elektronischen Zahlungssystemen der Partizipanden elektronischer Zahlungssysteme herausgearbeitet, sowie die Kriterien der Akzeptanz beschrieben. Die hieraus gewonnenen Erkenntnisse ermöglichen die Identifikation von kritischen Erfolgsfaktoren. Die Arbeit beschreibt vorhandene Zahlungssysteme, wobei die Bereiche Zahlungsprotokolle und Frameworks ausführlicher diskutiert werden.

Im Rahmen des Projekts ‘European Electronic Cash System (EECS)’ wird in dieser Arbeit ein Framework für die Abwicklung und Abrechnung von verschiedensten Zahlungsarten spezifiziert. Das entwickelte Rahmenwerk umfaßt sowohl die Funktionen und Zahlungsströme, als auch die benötigten Geschäftsprozesse und wird durch ein Grobdatenmodell der EECS-Plattform ergänzt.

Eine kritische Betrachtung sowie ein Ausblick schließen die Arbeit ab.

Abstract

Many Internet trends are oriented towards commerce transactions, that support business process and the exchange of goods and services. Today there is a bunch of systems and applications for segments of electronic commerce, especially for electronic payment systems, which are identified as critical for the successful spread of E-Commerce in the Internet. These electronic payment systems are the main interest of this thesis.

This thesis explains the special interests and motives for electronic payment systems of malls and other participants. Furthermore, an overview of the criteria for acceptance is given. By the result of this task it is possible to identify the most important facts for success. This work discusses existing payment systems and has a focus on payment protocols and frameworks.

In the scope of the ‘European Electronic Cash System (EECS)’ project this work proposes a framework for different payment mechanisms. This framework includes functions, flow of payments and the required business processes are defined. Finally a data modell of the EECS-platform is presented.

A critical reflection and an outlook concludes the work.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Das Internet entwickelt sich rasant, von der Präsentationsphase, über die von Interaktion geprägten Phase, hin zur transaktionsorientierten Phase. Die angestrebte transaktionsorientierte Phase ist geprägt durch den Austausch von und Handel mit Waren und Dienstleistungen. Unternehmen erkennen die Chancen der neuen Technologien für neue Geschäftsfelder, Vertriebswege und Absatzmärkte, mit Millionen von Online-Kunden, im Netz der Netze.

Neue Technologien eröffnen neue Möglichkeiten für die Gestaltung und Durchführung der Geschäftsprozesse innerhalb der Geschäftstätigkeit eines Unternehmens. Sind die Motive für eine Neu- bzw. Umgestaltung der Geschäftsprozesse aus der Verfügbarkeit neuer Technikinnovationen entstanden, bedingt dies einen Ansatz, der stark an der technologischen Machbarkeit ausgerichtet ist.

Dieser technikgetriebene Ansatz, bringt jedoch neben Verbesserungen auch eine Reihe von Problemen mit sich. So finden die betriebswirtschaftlichen Anforderungen für die Geschäftsabläufe kaum Berücksichtigung, was unweigerlich zum Medienbruch im Transaktionsablauf führt. Die Unterstützung durch IT-Mittel ist nicht für alle betriebswirtschaftlichen Abläufe vorhanden, bzw. wird durch den zum Teil unterschiedlich ausgeprägten Grad der Unterstützung mit inkompatiblen Techniken realisiert.

Desweiteren herrscht ein wahrer Wildwuchs an Systemen und Anwendungen für Teilbereiche des *Electronic Commerce* und speziell für den Bereich Zahlungssysteme, der als kritischer Erfolgsfaktor für die Verbreitung des E-Commerce im Internet eingestuft wird und Gegenstand dieser Arbeit ist.

Bis heute wurden sehr viele unterschiedliche Ansätze zur Realisierung von Zahlungssystemen im Internet erprobt und teilweise eingesetzt. Bisher hat sich jedoch noch kein unangefochtener Standard herausgebildet und es ist fraglich, ob die Vielzahl der Anbieter und Interessenverbände sich in naher Zukunft auf einen gemeinsamen Standard einigen können, bzw. ob die „Internetgemeinde“ einen Quasistandard etabliert. Es muß vielmehr davon ausgegangen werden, daß mehrere Zahlungssysteme nebeneinander existieren, wie beim „realen Geld“ ebenfalls, und ein Käufer auch mehrere Systeme anwendet, z.B. in Abhängigkeit von Transaktionsform bzw. -volumen. Dies bedeutet für den Händler, der im „Käufermarkt“ Internet Handel betreibt, daß er die verschiedensten Zahlungssysteme akzeptieren muß.

Die benötigte Infrastruktur hierfür ist, gerade von kleinen Händlern, unter Kosten-/Nutzengesichtspunkten nicht wirtschaftlich realisierbar. Anstatt in die Infrastruktur zu investieren, wird ein Dienstleister nachgefragt werden, der die Abwicklung verschiedener Zahlungsarten für den Händler übernimmt. Diese Dienstleistung kann z. B. von einer Mall oder aber von einem auf Zahlungsabwicklung spezialisierten Service-Unternehmen angeboten werden.

1.1 Zielsetzung der Arbeit

Vor dem Hintergrund von fehlenden Standards wird auf die speziellen Interessenschwerpunkte einer Mall (Kapitel 2) eingegangen, es werden die Motive für den Einsatz von elektronischen Zahlungssystemen (Kapitel 3) herausgearbeitet, sowie die Kriterien der Akzeptanz (Kapitel 4) beschrieben. Die hieraus gewonnenen Erkenntnisse ermöglichen die Identifikation der kritischen Erfolgsfaktoren (Kapitel 5). Die Arbeit baut auf vorhandene Zahlungssystemuntersuchungen (Kapitel 6) auf, wobei die Bereiche Zahlungsprotokolle und Frameworks ausführlich diskutiert werden.

Für die Firma 'European Electronic Cash System (EECS)' wird ein Rahmenwerk für die Abwicklung der Abrechnung von verschiedensten Zahlungsarten entwickelt, das als Konzept für die technische Spezifikation des IT-Gesamtsystems dient. Das Rahmenwerk umfaßt sowohl die Funktionen und Zahlungsströme, als auch die benötigten Geschäftsprozesse (Kapitel 7).

Um die Geldtransferprozesse der verschiedenen Zahlungssysteme abwickeln zu können, bedarf es einer offenen und ausbaufähigen Plattform, die die Funktionen, die Geschäftsprozesse und die von den Protokollen geforderten Daten zur Verfügung stellt. Ein Grobdatenmodell für eine solchen Plattform wird entwickelt (Kapitel 8). Dieses Grobdatenmodell dient als Spezifikationsgrundlage bei der Entwicklung der EECS-Applikation. Die gewonnenen Erkenntnisse werden Aufschluß darüber geben, ob und in welchem Umfang eine grundlegende, allgemein anwendbare Konzeption für die Abwicklung von unterschiedlichen Zahlungssystemen, innerhalb eines von einem Dienstleister betriebenen Gesamtsystems, möglich ist.

1.2 Aufbau der Arbeit

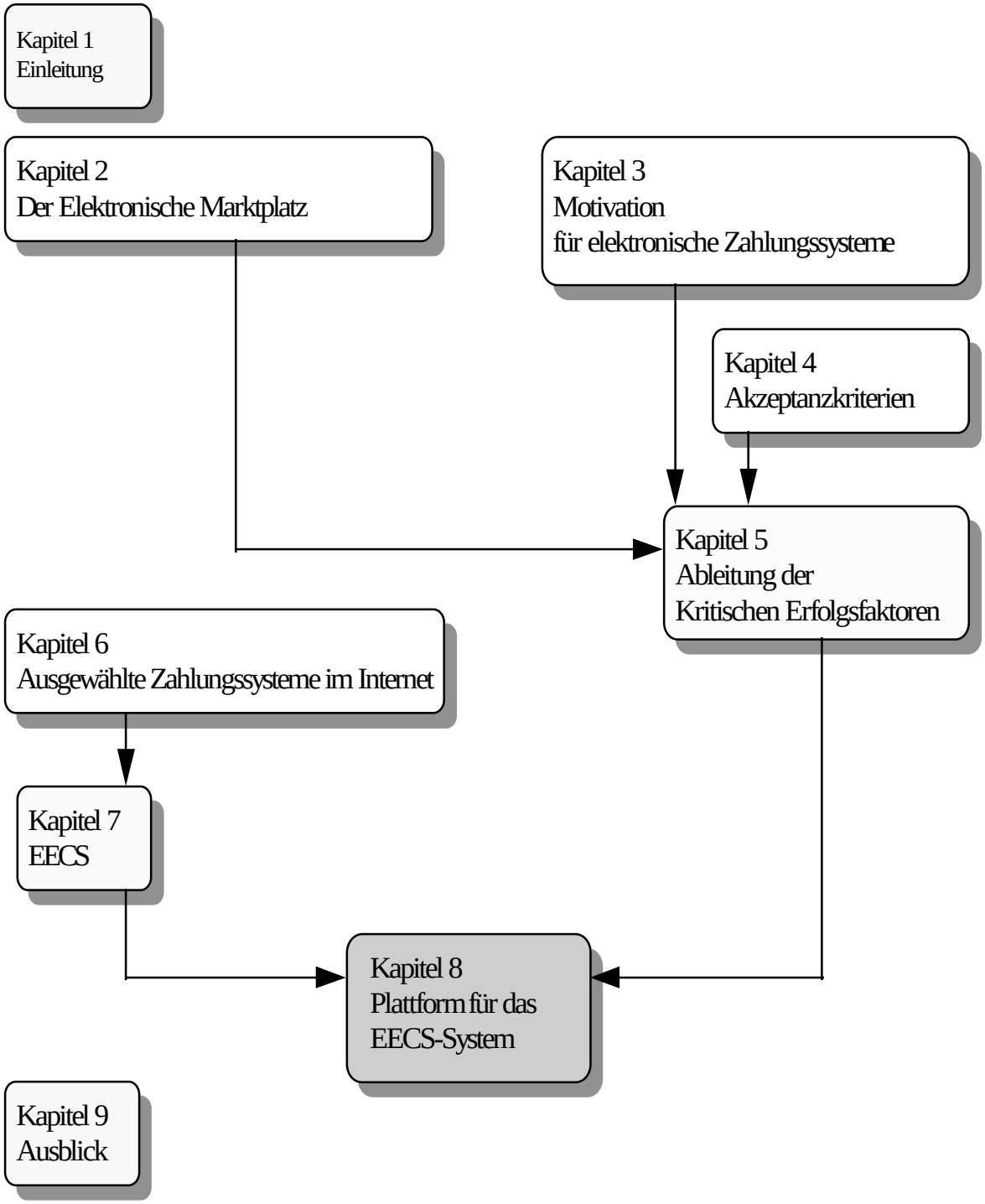


Abbildung 1-1; Aufbau der Arbeit

2 Der Elektronische Marktplatz

Die Organisationsform der elektronischen Märkte ist der elektronische Marktplatz. Die *Mall*, oder auch *electronic mall* wird synonym mit dem Begriff elektronischer Marktplatz verwendet.

Elektronische Marktplätze sind *„...die institutionellen konkreten Vermittlungsformen der elektronischen Märkte. Weiter wollen wir die Organisation elektronischer Dienste dann als Marktplätze bezeichnen, wenn sie zum einen für die Öffentlichkeit zugänglich sind und wenn sie zum anderen eine offene Palette an Dienstleistungen anbieten, sie also nicht auf ein spezielles Fachgebiet oder eine spezielle Anwendung beschränkt sind.*“ [Kuhl96, S. 51]

Kuhlen definiert unter anderem die Unterstützung aller Formen der Geschäftstransaktion, sowie das Ausmaß kommerzieller Interaktionsfunktionen, als Qualitätskriterien für einen elektronischen Markt [Kuhl95b]. Elektronische Zahlungssysteme bilden die zentrale Grundlage für eine durchgängige IT-Unterstützung der Geschäftstätigkeit im Internet, da sie Bestandteil der meisten Geschäftstransaktionen sind. Semar spricht in diesem Zusammenhang von „wahren virtuellen Marktplätzen“, die alle notwendigen Transaktionsformen unterstützen [Gö/Se97].

Kennzeichen elektronischer Märkte sind deren Unabhängigkeit von Raum und Zeit, sowie ihre außerordentliche Heterogenität, die sich in der Vielgestaltigkeit der Ansätze zum Aufbau elektronischer Märkte und dem Aufkommen proprietärer Systeme zeigt [Schm2/97].

2.1 Die elektronische Einkaufs- und Erlebniswelt

Das elektronische Einkaufen, oder neudeutsch *Online-Shopping*, ist nicht als die elektronische Kopie des bisher bekannten Einkaufsbummel zu sehen. Die Gestaltungsmöglichkeiten, die die elektronischen Medien zur Verfügung stellen, prägen das Online-Shopping und differenzieren es von der konventionellen Art einzukaufen. Diese Gestaltungsmöglichkeiten bergen ein großes Innovationspotential, das noch längst nicht ausgeschöpft ist. Ziel der Innovationen ist es, das Angebot an Waren und Dienstleistungen so zu optimieren, daß sich ein Mehr an Qualität und Zufriedenheit für Kunde und Anbieter ergibt [Was97].

In den nachfolgenden Abschnitten sollen Innovationspotentiale und identifizierbare Risiken eingehender diskutiert werden.

Bei den zur Zeit breit eingesetzten Darstellungsformen des Online-Shopping wird primär das Sehen und teilweise auch das Hören als Sinn angesprochen. Die Dominanz des Sehens geht aber einher mit einer Erstarrung des Sehens, da das Auge beim Blick auf den Bildschirm keine Akkomodationsleistung erbringen muß. Dieser „starre Blick“ auf den

Bildschirm kann eine einschläfernde oder sogar bewußtseinsverändernde Wirkung haben, ähnlich der Hypnose oder Trance [Budd96]. Es ist daher von besonderer Bedeutung die spezifischen Faktoren, die die Aufmerksamkeit und Konzentration des Benutzers beeinflussen, bei der Gestaltung der „Einkaufswelt“ zu berücksichtigen.

Der Konsument kann diese Reizüberflutung der Sinne Sehen und Hören, die sehr intensiv angesprochen werden, einhergehend mit einem Defizit an Reizen, die durch die übrigen Sinne, wie z.B. den Tastsinn, Geruchssinn etc., aufgenommen und verarbeitet werden können, als unbefriedigende oder unvollständige Erfahrung empfinden. Erst das Zusammenwirken der Sinne gibt dem Individuum das Gefühl von Sicherheit und ruft positive Assoziationen hervor, da eine Erfahrung als vollständig eingestuft wird hinsichtlich der erfahrenen Sinneseindrücke. Das Gefühl von Sicherheit entsteht dadurch, daß eine möglichst große Anzahl von gespeicherten Sinneseindrücken, die im Zusammenhang mit einer, in der Vergangenheit erfahrenen, ähnlichen Situation, den Sinneswahrnehmungen der momentanen Situation entsprechen und somit als *vertraut* eingestuft werden können. Das mit allen Sinnen erfahrene Einkaufserlebnis findet bisher noch nicht statt, da die elektronischen Medien nicht alle Sinne ansprechen können. Die Frage ist jedoch in welchem Umfang die Sinnesreize des realen auf das elektronische Einkaufserlebniss abbildbar, im Sinne einer exakten Kopie, sein müssen, obwohl es sich bei der Betrachtung um differente Medien handelt. Die Vorteile des Online-Shoppings, die in der realen Welt nicht realisierbar sind, können das Defizit an Sinnesreizen teilweise kompensieren.

Bestrebungen, dieses Defizit zu eliminieren, sind in der Virtual Reality (VR) Forschung erkennbar. VR versucht, mit immer ausgefeilteren Techniken und Gerätschaften (Datenhelm, Datenhandschuh, etc.), Sinnesreize und -eindrücke zu simulieren [Bull96]. Obwohl es durch die gesteigerte Rechnerleistung möglich ist das Verhalten von Objekten in einer natürlichen Weise nachzubilden, gelingt die totale Immersion [Patz96] noch nicht. Da die Sinneswahrnehmungen so vielfältig und vielschichtig sind, ist eine Imitation zu komplex, um sie mit den heute verfügbaren Datendurchsatzraten und Techniken identisch nachzubilden.

VR ist eine Vorstufe zur Wirklichkeit und dient als Realisierungsgrundlage in der Verkaufsunterstützung für Produkte, deren Vielfalt an Auswahlmöglichkeiten keine reale Präsentation zulassen, wie z.B. Fahrzeugbau, Küchen- oder Büroeinrichtungen. Einige VR-Internet-Shops[1], die künstliche Räume in ihren virtuellen Welten an Warenanbieter vermieten [GePo98], werben mit dieser Technologie, deren realisierte Umsetzung jedoch noch viele Wünsche offen läßt, da sie kaum über eine animierte 3D-Darstellung hinaus geht.

Unabhängig von den Entwicklungsfortschritten der VR-Technologien ist es essentiell wichtig, Mehrwerte zu generieren, da der Konsument das elektronische Einkaufserlebnis

[1] z.B. http://virtual.design-exhibition.com;
http://www.digital-city.de;
http://www.DieStadt.net;

nur dann als erstrebenswert und befriedigend empfinden wird, wenn er einen für ihn meßbaren Mehrwert ableiten kann, der das Fehlen einzelner Sinneswahrnehmungen kompensiert.

Ob und in welchem Umfang ein solcher Mehrwert generiert werden kann, ist unter anderem von dem individuellen Produkt respektive von der Dienstleistung selbst und desweiteren von deren Onlinepräsentation abhängig. Nicht jedes Produkt trägt diesen Mehrwert inhärent, so daß über die Produktdifferenzierung der Mehrwert umgesetzt werden kann. Beispiele sind primär Produkte, die in digitaler Form vorliegen, aber auch die oben erwähnten präsentationslastigen Produkte mit hohem Erklärungsaufwand, bei denen die Visualisierung zur Verdeutlichung der getroffenen Aussagen beiträgt.

2.2 Die Marktdienste

Die Beweggründe eines Internet-Nutzers eine Mall anzuklicken, sind vielfältig. Während der eine das breitgefächerte Angebot und die Informationsvielfalt schätzt, möchte der andere schnell und gezielt auf ein bestimmtes Produkt zugreifen. Beiden gemein ist der Wunsch nach individueller Bedürfnisbefriedigung und hierfür erwarten sie Dienste oder Agenten, die sie bedürfnisadäquat unterstützen. Das Angebot ist vielfältig, und genau diese **Vielfalt** ist der Ursprung für die Nachfrage nach einem Service, der das Angebot qualifiziert.

Die charakteristischen Eigenschaften der Malls ermöglichen dem Benutzer schon eine Vorabauswahl. Diese strukturierenden Charakteristika wie z.B. regionaler Bezug, Branchen, Produktgruppen, oder bei Informationsmärkten deren Klassifizierung[2], sowie die Möglichkeit innerhalb der Mall benutzerspezifische Sichten aus der Menge der Angebote zu generieren, erhöhen für den Benutzer den Grad der durchschnittlichen Relevanz.

Um benutzerspezifische Sichten erstellen zu können, bedarf es deduzierter Daten als Basis. Inwieweit Benutzerprofile *(**Profiling**)* für diese Unterstützung erstellt und vor allem gespeichert werden sollen, ist strittig. Datenschützer beunruhigt die hieraus resultierende Rückverfolgbarkeit der Aktionen jedes Benutzers [FuWr97]. Sie sehen die Sammlung dieser personenbezogenen Daten, über Konsumgewohnheiten und Verhaltensmuster, als Eingriff in die Privatsphäre des Anwenders. Die Gefahr des Mißbrauchs dieser Daten ist gegeben. Es kann nicht absolut sichergestellt werden, daß die kollektierten sensiblen Daten, stets nur mit legitimer Absicht und Kompetenz, ausgewertet werden.

Das aus dem *Profiling* abgeleitete personalisierte Serviceangebot *(**Matching**)* stellt für den Benutzer einen konkreten Mehrwert dar, da unter Berücksichtigung dieser Daten relevante Informationen aus der Informationsvielfalt benutzeradäquat aufbereitet werden können. Das Konzept des One-to-One-Marketing setzt auf diesem Potential auf und ermöglicht ein individualisiertes Marketing.

---

[2] Kuhlen unterscheidet fünf Klassen von Informationsmärkten (Fachkommunikation, Geschäftskommunikation, Verwaltungskommunikation, Publikumsmärkte und Individualmärkte) [Kuhl95a]

Der Zielkonflikt zwischen Betreuung und Eingriff in die Privatsphäre ist jedoch gegeben und sowohl als Chance als auch als Risiko zu identifizieren. Mit dem inzwischen gebräuchlichen Sinnbild des „gläsernen Menschen“ wird die Problematik des Sammelns von personenbezogenen Daten treffend beschrieben (vgl. Kap. 4.2).

Derjenige, der für etwas **bezahlt**, **kontrolliert** es auch. Die von Werbeanzeigen und Banner überfluteten Web-Sites sind die besten Beweise für diese These.

Jakob Nielsens These: *„...Ultimately, those who pay for something control it. Currently, most websites that don’t sell things are funded by advertising. Thus, they will be controlled by advertisiers and will become less and less useful to the users.“* [useit.com]

Für den Nutzer wird es jedoch auf diesen Sites immer schwieriger, seine Informationen zu filtern. Die Seiten werden im Hinblick auf marketingwirksame Strategien designt und nicht für einen Kunden, der schnell und effizient seinen Informationsbedarf decken möchte. Bezahlt der Webnutzer für die Seiten, die er abruft, wird der Anbieter auf seine Wünsche, die nun als Kundenwünsche relevant sind, eingehen.

Um diese Konzepte umzusetzen, können Micropayment-Zahlungssysteme eingesetzt werden. Der Anwender bezahlt bei Abruf die für ihn wertvollen Seiten und auch sporadische Benutzer können so, ohne umständliche Formalismen zu durchlaufen, wie z.B. Anmeldeformulare ausfüllen, Benutzer-Login anfordern, etc., das Angebot nutzen. Die im Vergleich zu Abonnements niedrigeren Eintrittsbarrieren forcieren die Nachfrage und erleichtern dem Interessenten den Erstkontakt mit dem Anbieter. Bei Abonnements muß der Nutzer im vorhinein festlegen in welchen Perioden oder Mengen er Informationen abnimmt. Der potentielle Abnehmer ist aber nicht immer bereit eine solche Verpflichtung einzugehen, zumal es nicht immer möglich ist den tatsächlichen Bedarf abzuschätzen.

Die schon erwähnte Informationsvielfalt wird unter anderem auch durch Communities, **Kommunikationsforen** für Kunden, erreicht.

„*Im Kontext der Online-Welt versteht man unter ... Gemeinschaft (community) ... jene soziale Einheit, in der Menschen leben, arbeiten und spielen. Mitglieder von Online-Gemeinschaften können ... durch Disskusionsforen interagieren.*“ [Dys98]

Den Kommunikationsforen im Internet ist gemein, daß sie die Bildung von Gemeinschaften erleichtern. In diesen Gruppierungen werden gemeinsame Interessen gepflegt und Ziele verfolgt. Unabhängig von der Geographie oder der Zugehörigkeit zu sozialen Schichten in der realen Welt, animieren diese „virtuellen Treffpunkte“ sich mit anderen auszutauschen.

Diese medial konstituierten „sozialen Welten“ stellen primär die Kommunikation und die Erstellung einer gemeinsamen Öffentlichkeit zur sozialen Unterstützung in den Vordergrund [Höf96]. Geeignete Methoden und Anwendungen müssen gefunden werden, um das Potential des Mediums [Kuhl2/98] so zu nutzen, daß unterschiedlichste

Formen des gegenseitigen Austauschs von Nachrichten, Meinungen, Klatsch und Tratsch etc. eine akzeptierte Plattform finden. Kommunikationsforen leisten einen Beitrag zur Kompensation des schwindenden persönlichen Kundenkontakts und fungieren als Begegnungszentren.

Die gemeinsame Öffentlichkeit und der Interessenverbund der Anbieter unter dem gemeinsamen Dach der Mall stellt für den Benutzer einen gewissen Schutz dar und schafft **Vertrauen**. Im Interesse der Mallbetreiber und der Anbieter wird Wert auf fairen Handel gelegt und es werden keine „schwarzen Schafe“ geduldet bzw. werden potentielle Teilnehmer im vorhinein geprüft. Dieser Aspekt ist nicht zu vernachlässigen, da es gerade in einem offenen Netz wie dem Internet schwierig ist, Kriterien für die Vertrauenswürdigkeit eines Anbieters auszumachen. Die Identifizierung mit der Mallgemeinschaft kann dem Händler einen Vertrauensbonus beim Kunden verschaffen.

Im Bereich der Netzpräsenz des Händlers werden gerade an die Shopping-Applikation hohe Anforderungen seitens der Kunden gestellt. Die Dynamik und Intransparenz des IT-Marktes tut ein weiteres, so daß die Shop-Software innerhalb kürzester Zeit nicht mehr State-of-the-art ist und Erweiterungen, ein Update oder gar eine Systemumstellung nötig sind, die Vorabinvestitionen und DV-technische Kompetenz bedingen, um konkurrenzfähig zu bleiben. Hieraus ergibt sich ein **Outsourcingpotential**, das sich auf Geschäftsprozesse erstreckt, die nicht als Kernkompetenzen bzw. Alleinstellungsmerkmal des Anbieters einzustufen sind. Vor diesem Hintergrund wird vom Händler eine Dienstleistung nachgefragt, die von Goebels als **Querschnittsdienstleitung** bezeichnet wird.

„Querschnittsdienstleitungen sind Funktionen, die von einem Markt zur Verfügung gestellt werden ... Das Mehrwertpotential begründet sich dabei in der universellen Verfügbarkeit dieser Dienstleistung...“ [Goeb97].

Als Querschnittsdienstleistungen eignen sich z.B.:

- Zahlungssysteme
- Warenkörbe
- statistische Auswertungen
- Abwicklung internationaler Steuer- und Zollformalitäten
- Kundenprofilanalysen (Customer Profiling)
- Distribution
- Communities
- Callcenter und Abonenntenverwaltung
- Suchsysteme

Um die Funktionalitäten der Querschnittsdienstleistungen in der Mall zur Verfügung zu stellen, kann die Komponenten-Technologie eingesetzt werden. Abbildung 2-1 veranschaulicht die Interaktion der Komponenten mit den mallweit angebotenen

Querschnittsdienstleistungen. Dieses Modell ermöglicht dem Händler in seinen Web-Seiten statische Anteile, aktive Komponenten und Sichten auf Objekt-Daten zu implementieren.

Zudem können auf diesem Wege **integrative Mehrwerte** für den Kunden des Händlers erzeugt werden. Zum Beispiel kann dem Kunden, der beim Fahrradhändler A ein Treking-Fahrrad ordert, eine Auswahl an Radwanderkarten der Region des Buchhändlers B, angeboten werden. Ähnlich wie bei der Kundenprofilanalyse kann für die Produkte ein Profil erstellt werden, das es ermöglicht über Matching passende Zusatzinformationen und -angebote, innerhalb der Produktpaletten der Händler des elektronischen Marktplatzes, anzubieten.

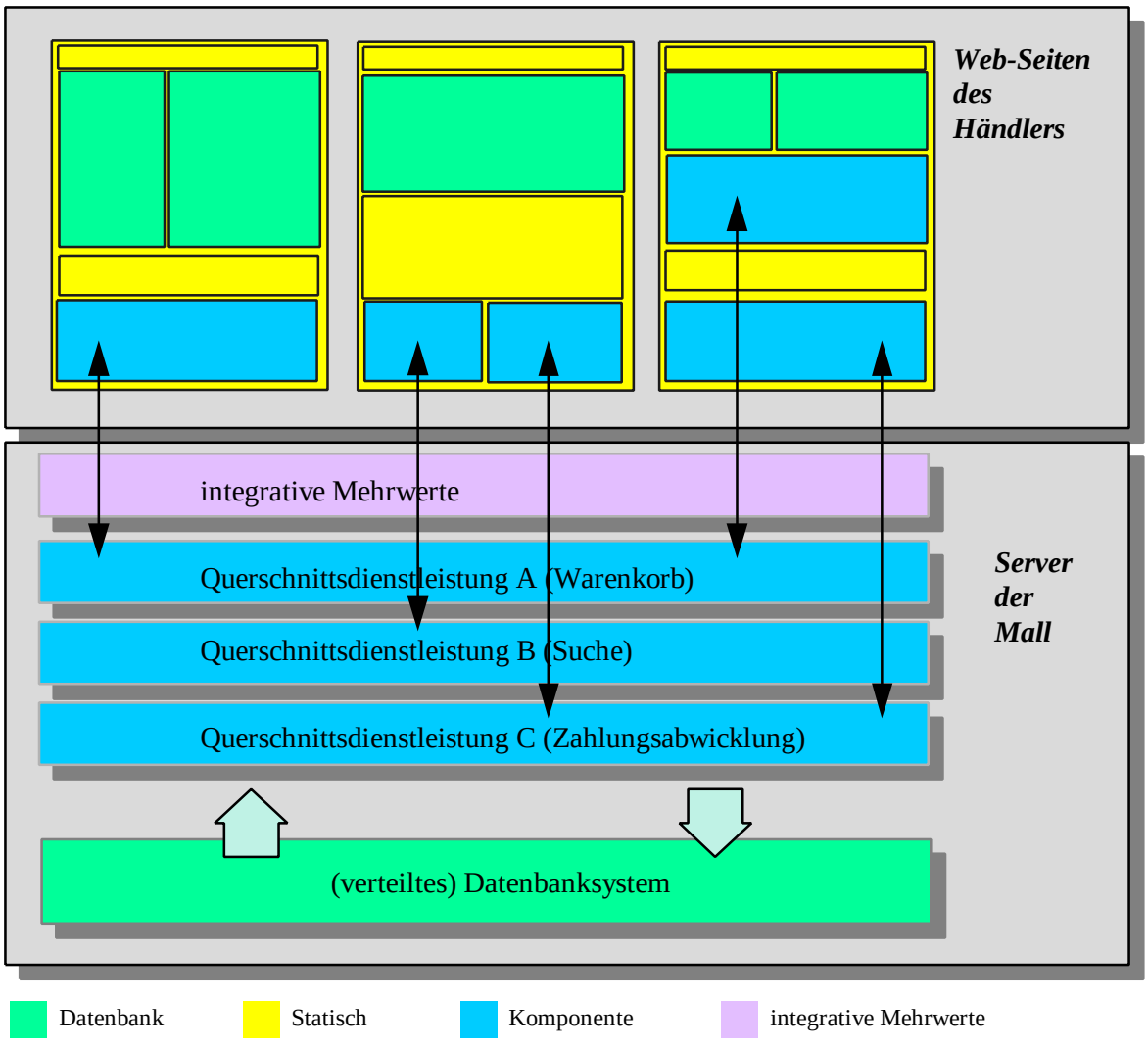


Abbildung 2-1; Querschnittsdienstleitungen

Bei der Querschnittsdienstleistung *Zahlungsverkehr* ist das Vertrauen in die Seriosität des Dienstleisters ein entscheidender Faktor. Der Einsatz zertifizierter Softwareprodukte und Standards sind Grundvoraussetzungen für das nötige Vertrauen der Kunden. Die Mall kauft sich diese Softwareprodukte, oder aber bietet diese Funktionalität über einen

Finanzdienstleister an. Sie stellt quasi einen Zahlungsserver, als mallweite Ressource für alle Zahlungssysteme, zur Verfügung.

Die **identifizierbaren Vorteile** beim Einsatz der Querschnittsdienstleistung Zahlungsverkehr sind:

⇒ aus **Käufer Sicht**:

- Das einmalige Bezahlen aller im Warenkorb befindlicher Produkte von unterschiedlichsten Händlern, birgt Vorteile hinsichtlich der Sicherheit und Transaktionszeit, da die Zahlungsdaten nur einmal übers Netz gesendet werden müssen. Zudem ist es für den Käufer bequemer und rationeller den Formalismus für den Bezahlvorgang nur einmal zu durchlaufen.
- Da nur eine Abbuchung auf dem Käuferkonto erfolgen muß, wird nur eine Buchungsgebühr fällig.
- Es werden eine Reihe unterschiedlichster Zahlungsmittel akzeptiert.
- Der Käufer hat die Gewährleistung der Mall-Organisation, daß die Zahlungsabwicklung durch ein vertrauenswürdiges System erfolgt.
- Die Mall stellt state-of-the-art Applikationen zur Verfügung.
- Der Käufer kann mittels einer durchgängige Bedienerführung für den Bezahlvorgang zugreifen.
- Bei Rückfragen und Reklamationen hat der Käufer einen Ansprechpartner, z.B. das Callcenter der Mall, als *single-point-of-contact*.

⇒ aus **Händler Sicht**:

- Der Händler hat einen Vertragspartner für die Abwicklung des Zahlungsverkehrs. Komplikationen, die sich aus Schnittstellen- oder Kommunikationsproblemen ergeben können, sind somit minimiert.
- Die Einschränkung des Kundenpotentials wegen inkompatibler Zahlungsmittel ist auf ein Minimum begrenzt, da die Zahlungsabwicklung der Mall ein größeres Angebot an Zahlungsmethoden ökonomisch vertretbar anbieten kann.
- Die Fremdwährungsabwicklung wird von einem Dienstleister übernommen.
- Der Händler partizipiert an den günstigen Konditionen für die Zahlungsabwicklung. Diese Konditionen können auf Grund des Transaktionsvolumens (z.B. bei Kreditkartenabrechnung) oder anderer Umsatzdaten gewährt werden.
- Eine einheitliche Schnittstelle zum Zahlungsmodul erleichtert dem Händler die Integration in seine bestehenden Anwendungen.

- Die Mall stellt den prompten Einsatz neuer Zahlungsmodule sicher. Für den Händler entsteht kein Update- und Wartungsaufwand.
- Für den Händler entsteht kein risikobehafteter Vorabinvestitionsbedarf.

2.3 Zusammenfassung

Schmidt beschreibt die Vision von einem integrierten **globalen Marktplatz** als eine „...*Art Basar, auf dem der Kunde auf Verlangen alle Angebote der Welt präsentiert erhält - in wenigen Jahren auch in photorealistischer virtueller Realität ‚wo er auf Knopfdruck bestellen, bezahlen und seine Leistung absetzen kann"* [Schm10/97]. Das Netz als Plattform für die Abwicklung aller Aufgaben - ein virtueller Supermarkt von unvorstellbarer Dimension.

Angesichts dieser Vision, sollten die Risiken der „schönen neuen Welt" nicht unbeachtet bleiben. Gravierende Änderungen der **Wahrnehmung** und im sozialen Verhalten der Konsumenten sind durch den Einsatz und Gebrauch der neuen Technologien wahrscheinlich. Die Auswirkungen dieser **Verhaltens- und Kommunikationsänderungen** sind zur Zeit nicht vollständig abzusehen.

Der elektronische Handel wird aber die etablierten, althergebrachten Handelsformen nicht vollständig ersetzen, sondern ergänzen - ergänzen in den Bereichen, die dafür besonders geeignet sind, bzw. die durch den elektronischen Handel erst ermöglicht werden (vgl. Kap. 3.2; globale Angebotspalette).

Die Motive, das *Online-Shopping* und den *Online-Handel* über die Organisationsform elektronischer Marktplatz abzuwickeln sind vielfältig. Der Vertrauensbonus und die hohe Orientierungs-, Such-, Navigations- und Selektionsleistung von elektronischen Marktplätzen, sind wohl die vorrangigsten Beweggründe [Kuhl95b].

Um ihr gesamtes Potential ausspielen zu können, brauchen elektronische Märkte geeignete, sichere Zahlungsformen und -mittel. Im heutigen verschärften Wettbewerb, differenzieren sich Unternehmen nicht nur über Produkte und Preise, sondern immer mehr über die Qualität ihres gesamten Leistungssystems [MuÖs98]. Die Mall als gemeinsamer Aktionsraum verschiedenster Händler bietet die ideale Basis zur Unterstützung dieser Systeme. Über **Querschnittsdienstleistungen**, die von der Mall angeboten werden, wird das elektronische Leistungsspektrum des Händlers kompletiert und es werden Mehrwerte für Käufer und Händler generiert.

3 Motivation für elektronische Zahlungssysteme

Im Kontext des Electronic Commerce werden die elektronischen Zahlungssysteme als „Enabling technology“ eingestuft. Im Netz verfügbare elektronische Zahlungsmittel können den durchschlagenden Erfolg des Electronic Commerce initiieren.

Alleine für den europäischen Markt wird, von der Studie „Europe’s Internet Growth“ der Forrest Research Inc., eine Steigerung des Online-Umsatzvolumens von 1,2 Milliarden Dollar in 1998 auf 64,4 Milliarden Dollar im Jahre 2001 prognostiziert. Mit 56,7 Milliarden Dollar fällt der Löwenanteil auf den Geschäftsverkehr, der Verbraucherhandel schlägt mit 4,6 und der Handel mit Informationen mit 3,1 Milliarden Dollar zu Buche [CW4/98].

Der hohe Stellenwert der Zahlungssysteme läßt sich auf deren Schlüsselposition in den Phasen der Markttransaktionen zurückführen. Markttransaktionen laufen in den Phasen Information, Abschluß und Abwicklung ab, wie in Abbildung 3-1 dargestellt. Zahlungssysteme sind, zusammen mit der eigentlichen Warenlieferung, Logistik und Kundendienst, der Abwicklungsphase zuzuordnen [LiRu97].

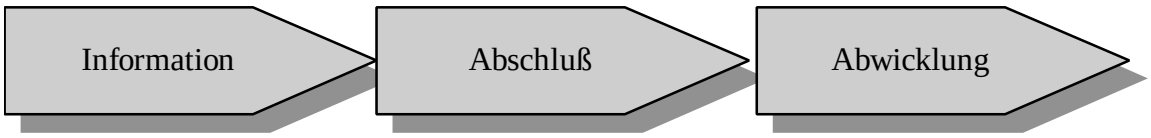


Abbildung 3-1; Phasen der Markttransaktion

Zur Vermeidung eines Medienbruchs in der Prozesskette muß eine durchgängige Unterstützung der Markttransaktionen über alle Phasen gegeben sein [Zimm97]. Erst mit der Verfügbarkeit von elektronischen Zahlungssystemen im Internet entstehen symmetrische Marktbeziehungen und der „Schaufensterbesucher“ wird zum Kunden [Siet97].
Außerdem hat die Durchgängigkeit der IT-Unterstützung unter dem Aspekt der produktspezifischen Herstellungsprozesse für Informationsgüter eine neue Dimension. Die ohnehin elektronisch entwickelten, produzierten und angebotenen Produkte und Dienstleistungen intendieren IT-Technologien [Kuhl95b].

Alleine die Verfügbarkeit von Systemen reicht jedoch nicht aus. Es wird davon ausgegangen, daß erst durch die breite Akzeptanz von elektronischen Zahlungssystemen das tatsächliche Geschäftsaufkommen im Internet die schon seit einiger Zeit prognostizierten hohen Werte erreicht. Diese Akzeptanz ist durch die Berücksichtigung der Motivationsgründe für elektronische Zahlungssysteme der Teilnehmer erreichbar. Als Teilnehmer können Händler, Käufer und Banken auf Grund ihrer unterschiedlichen Rollen innerhalb einer Markttransaktion unterschieden werden.

3.1 Motive der Händler

Der Begriff Händler ist in dieser Arbeit nicht auf die Bedeutung eines Handel Betreibenden reduziert, sondern wird synonym mit Anbieter von Waren und

Dienstleistungen verwendet. Der Händler wird als Marktteilnehmer in einem Handlungssystem mit geordneten Marktprozessen verstanden [vgl. Schn93 S.77].

Aus dieser Sichtweise erscheint die Betrachtung, der Einsatzbereiche für elektronische Zahlungssysteme, anhand der betriebswirtschaftlichen Funktionen im Marktprozess, sinnvoll [Schn97]. Das **Unterstützungspotential** der elektronischen Zahlungssysteme, das sich aus dem Einsatzbereich und dem Grad der Unterstützung ergibt, wurde in primär, also direkt zuzuordnen, und sekundär unterteilt. Jede betriebswirtschaftliche Funktion hat auf Grund ihrer Eigenschaften und Ausprägung andere Anforderungen an die IT-Mittel und deren Einsatz, hieraus ergeben sich die unterschiedlichen Potentiale für die Unterstützung. Durch die gewählte Darstellungsform in Abbildung 3-2, die sich an der Darstellung der „Wertkette“ [Schi95] orientiert, kann verdeutlicht werden, daß Wertschöpfungspotential vorhanden ist.

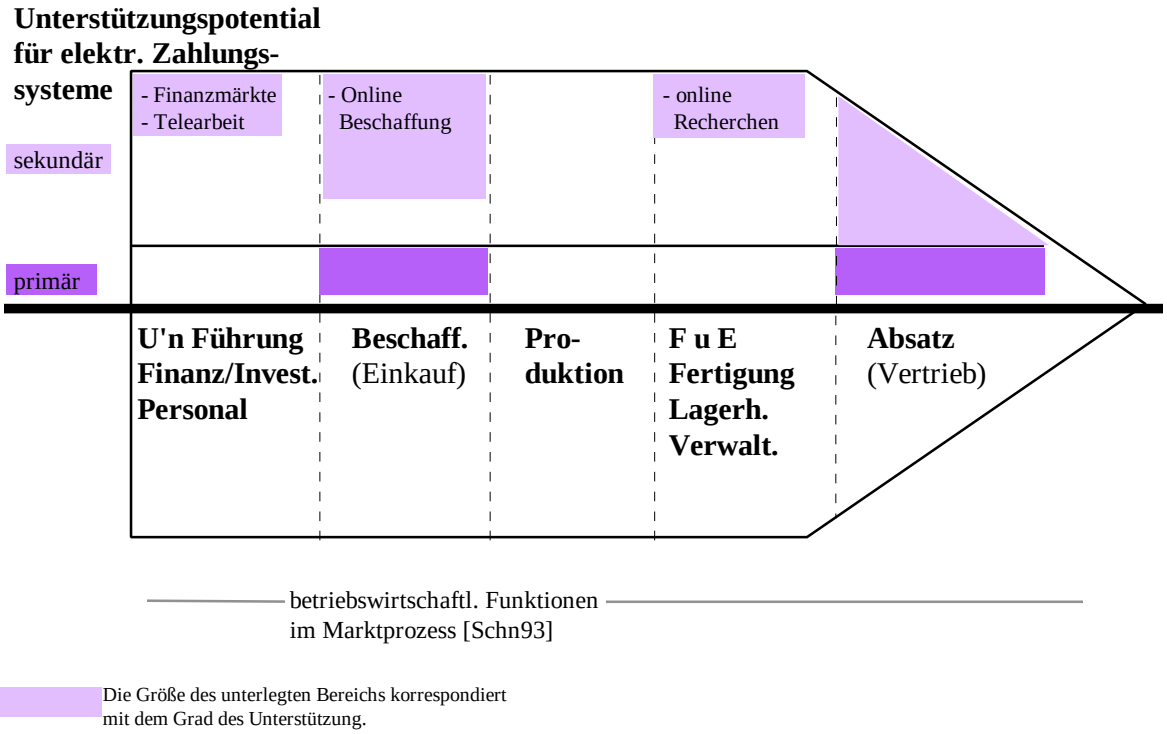


Abbildung 3-2; Prozesskette des Händlers

Die Quantifizierung des Unterstützungspotentials ist nur unter Berücksichtigung der speziellen Ausprägung und Vermarktbarkeit eines Produkts oder einer Dienstleistung sinnvoll.

Online vermarktbare Dienstleistungen und Produkte lassen sich unterteilen in die Kategorien *materiell*, hier muß die Lieferung der Produkte bzw. die Erbringung der Dienstleistung offline erfolgen, und *immateriell*, hier kann Lieferung bzw. Service online erfolgen. Handelt es sich um materielle Objekte, stellen die elektronischen Zahlungssysteme eine komfortable Alternative zur konventionellen Zahlungsmethoden dar. Dies gilt besonders für die Konditionen Anzahlung und Lieferung gegen Vorkasse.

Für immaterielle Objekte hingegen ermöglichen digitale Zahlungssysteme die Realisierung ganz neuer Geschäftsmodelle, die den besonderen Merkmalen von Information, Unterhaltung und Software gerecht werden [Siet97].

Für Unternehmer ist die Einrichtung einer ***Online Geschäftsabwicklung*** nur dann lukrativ, wenn ein gangbarer Weg existiert, aus dem Angebot über das globale Netzwerk, finanziellen Nutzen zu ziehen [FuWr97]. Primär ist der Händler an der Wirtschaftlichkeit seiner Internetpräsenz interessiert. In diese Wirtschaftlichkeitsbetrachtung fließen verschiedenste Faktoren ein, wobei im folgenden nur auf die Determinanten eingegangen wird, die aus dem Einsatz von Zahlungssystemen abgeleitet werden können.

Die **Determinanten** sind:

- Integration in den Geschäftsprozess
- Erschließung neuer Kundenpotentiale
- Kundenbindung durch Analyse des Einkaufsverhaltens
- Optimierung der Vertriebsstruktur
- Einbindung in bestehende Anwendung
- niedrige Kosten
- Risikominimierung

Integration in den Geschäftsprozess über definierte Standards;
Für Wirtschaftsunternehmen steht der Integrationsaspekt von elektronischen Zahlungsmitteln im Vordergrund. Die Einbindung im Sinne des Workflow-Gedanken macht eine Neuerfassung der Zahlungsdaten überflüssig und birgt die Vorteile [BusMed96]

- Kostenersparnis
- Zeitersparnis
- Fehlerreduktion

Erschließung neuer Kundenpotentiale durch die Erweiterung der Angebotspalette hinsichtlich neuer Dienstleistungen und informationstechnologisch unterstützter Transaktionsabwicklung;
Der Händler strebt an, zu einem frühen Zeitpunkt auf veränderte Bedürfnisstrukturen der Online-Shopper einzugehen, um diese Käufergruppe mit als erster ansprechen zu können und so den „Pioniervorteil“ als Alleinstellungsmerkmal gegenüber der Konkurrenz und als Werbepotential zu nutzen. Um keine potentiellen Kunden wegen inkompatibler Zahlungsmittel auszugrenzen, wird die Bereitstellung möglichst vieler akzeptierter Internet-Zahlungsmittel angestrebt. Es besteht die Forderung, möglichst alle erprobten Internet-Zahlungsmittel annehmen zu können, wobei nur ein geringer bzw. kein Aufwand bei der Implementierung entstehen sollte [Grun97].

Kundenbindung durch Analyse des Einkaufsverhaltens der Online-Shopper, zur Datenauswertung für den zielgerichteten qualifizierten Einsatz von Marketinginstrumenten und Kundenbindungssystemen;
Kundenbindungssysteme verfolgen die „Ziel-Triologie“:

- bestehende Kunden halten
- neue Kunden werben
- ehemalige zurückgewinnen

und qualifizieren die Daten, die über das Profiling gewonnen werden [Ara97].
Die Qualifizierung drückt sich aber auch in der effizienteren Gestaltung der individuellen Marketingaktionen aus, im Vergleich zum Massenmarketing. Einer der Vorteile des *WWW (World Wide Web)* liegt in der direkten Kommunikations- und Interaktionsmöglichkeit mit dem Kunden, d. h. der Händler kann auf die Bedürfnisse und Interessen des Kunden individuell eingehen [Was97]. Über die Kundenpersonalisierung kann der Händler die Kundengewohnheiten kennenlernen und individuell abgestimmte Dienstleistungen anbieten. Das ist unter der Kosten/Nutzen-Betrachtung sinnvoll, vor allem aber erschwert es die Etablierung eines Neueinsteigers, da die Kunden den Service erwarten und der Neueinsteiger die nötigen Kundenprofile noch nicht ermitteln konnte [O'Nei98]. Unter diesen Voraussetzungen kann der Händler seine Position im Markt, gegenüber neuen Konkurrenten, verteidigen.

Optimierung der Vertriebsstruktur oder der Vertriebswege;
Das Internet-Shopping ist besonders interessant für den Direktvertrieb der Hersteller, die nun auf ein kostenintensives Filialnetz verzichten und Kosteneinsparungen in der Distribution realisieren können. Handelsunternehmen müssen in diesem Kontext neue Konzepte entwickeln, die die Vorteile des Internet nutzen und den Konsumenten trotzdem so an das Unternehmen binden, daß er seine Entscheidung nicht nur auf Grund des Preises fällt [Luk97]. Zusatznutzen und spezielle Dienstleistungsangebote werden nachgefragt.

Einbindung in bestehende Anwendung der Unternehmens-IT;
Der Händler erwartet von den Zahlungssystemen die Möglichkeit der einfachen Adaption oder der Einbindung über definierte Schnittstellen an seine Hard- und Software-Ausstattung. Dies kann z.B. durch die Übernahme der Zahlungstransaktionsdaten in die Finanzbuchhaltung erfolgen, wie dies mittels EDI[3] schon seit mehreren Jahren im Business-to-Business-Bereich ohne Medienbruch erfolgt, oder als Anbindung an das Warenwirtschaftssystem des Händlers realisiert sein, um nur einige Beispiele zu nennen. Die Portabilität und Systemoffenheit korrespondieren eng mit dem ersten Punkt dieser Aufzählung „Integration in den Geschäftsprozess“.

niedrige Kosten für Zahlungsabwicklung;
Die Kosten für die Zahlungsabwicklung setzen sich zusammen aus den Zahlungstransaktionskosten mit eher variablem Charakter, die für jede Transaktion berechnet werden und den meist fix gestalteten Zahlungssystemkosten, die für die

[3] EDI (**E**lectronic **D**ata **I**nterchange); Elektronischer Datenaustausch

grundsätzliche Teilnahme am Zahlungssystem entrichtet werden. Desweiteren sind Kommunikations- und Administrationskosten genauso zu berücksichtigen wie die Preisgestaltung des Serviceangebots der Banken, die z.B. für beleghafte Aufträge weitaus höhere Bearbeitungsgebühren ansetzen als für Aufträge im standardisierten Austauschformat EDIFACT[4].

Risikominimierung durch Deckungsprüfung und Steuerung des Zahlungszeitpunktes;

Die Online-Autorisierungsanfragen bei einigen elektronischen Zahlungssystemen ermöglichen eine sofortige Deckungsprüfung, die einen gewissen Schutz vor zahlungsunwilligen bzw. unfähigen Kunden gewährleistet. Der Anbieter geht also nur dann in Vorleistung, wenn die Zahlung mit größter Wahrscheinlichkeit erfolgt. Der Zahlungszeitpunkt, der sich auf die Zeit zwischen dem Auslösen einer Zahlungstransaktion und der tatsächlichen Gutschrift auf dem Händlerkonto bezieht, nimmt ebenfalls Einfluß auf die Risikominimierung. Der Händler wird *pre-paid* (der Zahlungszeitpunkt liegt vor dem Kaufzeitpunkt) bzw. *pay-now*-Systeme (Kauf- und Zahlungszeitpunkt sind gekoppelt) favorisieren, da er bei diesen Systemen von einer umgehenden Kontogutschrift ausgehen kann. Die schlechte Zahlungsmoral von Kunden kann für viele, meist kleinere Unternehmen, eine existentielle Bedrohung darstellen.

[4] EDIFACT (**E**lectronic **D**ata **I**nterchange **f**or **A**dministration, **C**ommerce and **T**ransport); Internationaler Standard für den elektronischen Austausch kommerzieller Daten in einheitlichen Formaten für die Geschäftsvorfälle.

3.2 Käufer

Das Internet ist längst über die Startphase hinausgewachsen, in der das Netz hauptsächlich als Forschungsszenario diente und eine Fülle an Informationen kostenlos zur Verfügung gestellt wurde. Hatten die Internetnutzer der „ersten Stunde“ anfangs noch Schwierigkeiten kostenpflichtige Informationsangebote zu akzeptieren, ist der Benutzer heute durchaus bereit, für Informationen und Service zu bezahlen - vorausgesetzt sie repräsentieren für ihn einen Wert, bzw. befriedigen ein Bedürfnis.

Der ***Customer Bying Cycle*** (CBC) [Mau90] unterstützt das Erkennen von Kundenbedürfnissen und möglichen Formen der IT-Unterstützung [MuÖs98]. In Anlehnung an den *CBC* wird in der in Abbildung 3-3 dargestellten Prozesskette das primäre als auch das sekundäre Unterstützungspotential von Zahlungssystemen identifiziert. Auch hier wurde die Darstellungsform der Wertkette gewählt.

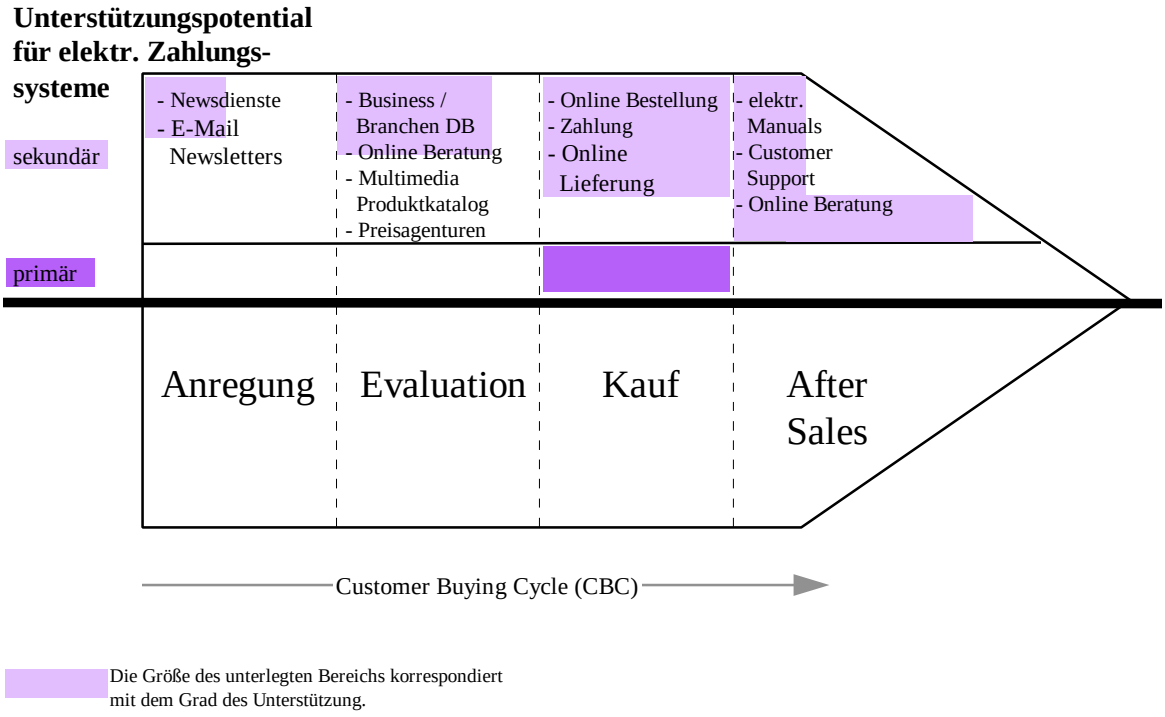


Abbildung 3-3; Prozesskette des Käufers

Kostenpflichtige Güter und Dienstleistungen werden also im Internet angeboten und nachgefragt. Für die Abwicklung der Kauftransaktion kommen elektronische Zahlungssysteme zum Einsatz. Einige Angebote sind exklusiv dem elektronischen Medium vorenthalten und manche Anbieter setzen die Internet-Zahlungsfähigkeit des Kunden einfach voraus. Will man als Käufer am E-Commerce teilnehmen und das breite Spektrum des Internetangebots nutzen, muß man über ein elektronisches Zahlungssystem verfügen.

Durch den Einsatz von elektronischen Zahlungsmitteln können dem Käufer sowohl Vor- als auch Nachteile entstehen, wie schon im vorigen Kapitel, sollen hier die **Determinanten** dargelegt werden:

- Kosten
- effiziente Preis- und Angebotsvergleiche
- Einsatz von „Intelligenten Agenten“
- globale Angebotspalette
- Währungsumrechnung
- Verfügbarkeit / Bequemlichkeit
- optionale Anonymität
- zeitsparende Abwicklung von Routinetätigkeiten
- Sicherheit durch definierte Geschäftsprozesse
- Benutzerfreundlichkeit
- universelle Akzeptanz
- kein Medienbruch

Kosten;
Für den Transfer von Zahlungen fallen die unterschiedlichsten Kostenarten an, die bei der Betrachtung des Kosten/Nutzen-Verhältnisses mitberücksichtigt werden müssen. Es sind dies im Einzelnen [BusMed96]:

- Registrierungskosten
- Kontoführungs- und Kontoauszugsgebühren
- Zahlungstransaktionskosten
    - ∞ Kosten des Mittlers
    - ∞ Kosten des Finanzintermediärs[5]
    - ∞ Kosten für die Kommunikationsverbindung

In der Regel entscheidet die Höhe der Zahlungstransaktionskosten und natürlich der Wert des Wirtschaftsgutes darüber, ob eine Zahlung ökonomisch sinnvoll abgerechnet werden kann. Zeitintensive Transaktionen erhöhen die Kosten für die Kommunikationsverbindung und sind zudem unbequem. Schnelle Verarbeitung und niedrige Transaktionskosten erhöhen die Benutzungsfrequenz eines Systems, da sie den Einsatz auch für kleinere Verrechnungsbeträge begünstigen [FuWr97].

[5] Vermittler in einer Finanztransaktion

Dem Käufer sollten alternative Gebührenmodelle angeboten werden, für die er sich, abhängig von seinen individuellen Nutzungsgewohnheiten, entscheiden kann. Eine monatliche Grundgebühr in Verbindung mit transaktionsabhängigen Kosten oder eine Pauschalgebühr, die das gesamte Transaktionsaufkommen abdeckt, wären mögliche Modelle.
Der Zeitpunkt der Zahlung muß in die Kostenbetrachtung mit einfließen, wobei der Käufer aus wirtschaftlichen Gründen mehr zu einer *post-paid* (der Zahlungszeitpunkt liegt nach dem Kaufzeitpunkt) als zu einer *pre-paid* -Lösung tendieren wird.

effiziente Preis- und Angebotsvergleiche;
Die Durchgängigkeit der IT-Technologie ermöglicht eine umfassende und zeitsparende Gegenüberstellung von Angeboten und Preisen. Der Markt wird transparenter durch differenzierte und dynamische Preismechanismen [Kam97].

Zum Teil wird jedoch die gewonnene Markttransparenz durch die Informationsvielfalt wieder überdeckt. Hinter dem Schlagwort *Information-Overflow* verbirgt sich die Problematik, trotz bzw. gerade wegen der hohen Quantität an Informationen, den Informationsbedarf nicht befriedigend decken zu können. Auf Grund der Vielzahl an Information ist es schwierig, einen Überblick zu bekommen und die *relevante Information* zu filtern.

Einsatz von „Intelligenten Agenten“;
Software-Tools wie die sogenannten *Intelligenten Agenten* können teilweise autonom Aufgaben für den Benutzer übernehmen. Der *„BargainFinder“* von Anderson Consulting z.B. sucht in einer Vielzahl von *Online-Musik-Shops* selbständig das billigste Angebot zu einer bestimmten CD [Kam97]. Mit Hilfe dieser Software-Technologie kann der Käufer dem *Information-Overflow* entgegenwirken und außerdem Routinetätigkeiten automatisch ausführen lassen.

globale Angebotspalette;
Das globale Netz als Basis für die elektronische Geschäftsabwicklung ermöglicht es dem Kunden seine Recherche für ein Produkt oder eine Dienstleistung weltweit durchzuführen. Dieser Produktvergleich kann zum einen Preisvorteile bringen. Zum anderen können Produkte geordert werden, die evtl. im Inland nur schwer oder gar nicht beschafft werden können, da der Anbieter hier keinen Vertrieb bzw. keine Repräsentanz unterhält.

Währungsumrechnung;
Komfortable elektronische Zahlungssysteme sollten dem Kunden ein einfaches Bezahlen in den verschiedensten Währungen ermöglichen. Dem Kunden sollte kein Aufwand durch Währungsumrechnung und kein Verlust durch Umtausch in bzw. von Fremdwährung entstehen.

Verfügbarkeit / Bequemlichkeit;
Der Käufer hat rund um die Uhr Zugriff auf das Angebot. Eine solche Verfügbarkeit von 24 Stunden an 365 Tagen im Jahr ist auch durch die großzügigsten Ladenöffnungszeiten nicht zu erreichen. Neben der zeitlichen ist vor allem die örtliche

Unabhängigkeit ein entscheidender Motivationsfaktor, der es erlaubt Geschäfte bequem von jedem beliebigen Ort aus zu tätigen [Bir98].

Die Bequemlichkeit erstreckt sich auch auf den Umstand, daß auf das gewohnte *Online-Einkaufsumfeld* nicht verzichtet werden muß. Trotz unterschiedlichster geographischer Aufenthaltsorte kann der Käufer in „*seiner Mall*“ oder bei „*seinem Händler*“ einkaufen und auf die bekannte Produktpalette oder den bewährten Service zurückgreifen.

optionale Anonymität;
Falls der Kunde seine Identität dem Verkäufer gegenüber nicht zeigen will, kann er durch den Einsatz eines geeigneten Zahlungsmittels anonym bleiben. Das Verbergen der Identität muß nicht zwangsläufig auf Motive hinweisen, die aus illegalen oder gar kriminellen Tatbeständen resultieren, vielmehr ist der Wunsch, die individuellen Kaufgewohnheiten nicht publik zu machen, aus Gründen des Persönlichkeitsschutzes, gut nachvollziehbar.

zeitsparende Abwicklung von Routinetätigkeiten;
Der von Vielen als lästig empfundene Einkauf von Lebensmitteln oder Dingen des täglichen Verbrauchs, stellt eine Routinetätigkeit dar. Für Konsumenten, die eine bequemere Alternative zur Hetzjagd zum Supermarkt kurz vor Ladenschluß suchen oder nicht mehr gewillt sind, samstags im Stau in Richtung Einkaufspark zu stehen, wurden bereits Konzepte entwickelt und pilotiert. Der Ablauf sieht vor, daß der Kunde über das Internet seine Bestellung aufgibt und die Waren innerhalb eines Zeitfensters geliefert bekommt, bzw. diese ähnlich einem individuellen Versorgungspaket abholt. Werden die Pakete zur Abholung bereitgestellt, bedarf es einer Infrastruktur, ähnlich eines Depots. In diesem Depot würden sich schließfachähnliche Einheiten befinden, die über einen speziellen Zugangscode oder ein Passwort vom Käufer geöffnet werden können. Im Lebensmittelhandel müßten die Fächer evtl. gekühlt werden, damit die Ware nicht verdirbt. Der Ansatz einer Pilotprojektidee, der recht vielversprechend zu sein scheint, nutzt das bestehende Tankstellennetz als quasi Auslieferungsdepot.
Ein für die Zukunft prophezeiter barcodelesender Kühlschrank, der die Bestellungen automatisch an den „Frischdienstprovider“ schickt, stellt den nächsten logischen Schritt in der Entwicklung dar.

Sicherheit durch definierte Geschäftsprozesse;
Die teilweise starr definierte Struktur der Transaktionsabläufe birgt für den Käufer auch eine gewisse Sicherheit. Der Käufer kann Einfluß nehmen auf die Einhaltung der Ablaufstruktur, z.B. hinsichtlich der Beweisbarkeit über erbrachte Leistungen oder Haftungsfragen, die nach den Gesichtspunkten des fairen Handels sichergestellt sein sollten[6].
Sind die Benutzer über die Gestaltung der Geschäftsprozesse und deren Ablauf informiert, könnte sich das Betrugs- und Verlustrisiko vermindern.

---

[6] Der Hackerangriff auf T-Online im März 1998 [spie30/3/98] hat einmal mehr gezeigt, daß eine Umkehr der Beweislast, wie von Kunden und Verbraucherverbänden gefordert, angezeigt ist. Der Anbieter sollte bei Unstimmigkeiten beweisen müssen, daß der Kunde die berechnete Dienstleistung auch tatsächlich in Anspruch genommen hat, und nicht umgekehrt.

Benutzerfreundlichkeit;
Das Zahlungssystem sollte über eine ergonomisch gestaltete, intuitiv zu bedienende Benutzeroberfläche verfügen, die den Qualitätsanforderungen für benutzerfreundliche Software-Applikationen genügen, und außer diesen Kriterien Zusatzfunktionen anbieten, wie z.B.:

- garantierte, möglichst automatische Updates
- Help-Hotline zum Zahlungssystembetreiber oder Call-Center für Individualberatung
- Online-Hilfesysteme
- Unterstützung von Chat- und Newsgroups-Aktivitäten

universelle Akzeptanz;
Die universelle Akzeptanz des Zahlungssystems bei Finanzinstitutionen und Verkaufsstellen ist ein Initialkriterium für elektronische Zahlungssysteme [Pern97]. Bei der Entscheidung für ein Zahlungssystem wird der Online-Shopper die Akzeptanz mit hoher Priorität berücksichtigen, da die Forderung nach „...Zahlung mit einem Zahlungsmittel der eigenen Wahl und zwar unabhängig vom Händler“ [Grun97] noch nicht realisiert ist.

kein Medienbruch;
Der Käufer im Internet fordert die Durchgängigkeit der IT-Unterstützung von der Kontoeinrichtung über den Geldtransfer bis hin zur eigentlichen Zahlung. Medienbrüche, wie z.B. die Übermittlung besonders schutzwürdiger Konto- bzw. Kreditkartendaten via Fax oder Telefon, wie dies beispielsweise von First Virtual[7] teilweise praktiziert wird, können als störend empfunden werden. Nichts desto trotz nimmt der Internetnutzer den entstehenden Aufwand hierfür in Kauf.

[7] http://www.fv.com

3.3 Banken

Die Banken sind, wie andere Wirtschaftsunternehmen auch, an einer kostengünstigen Abwicklung ihrer Transaktionen interessiert und suchen nach Innovationen, die es ihnen erlauben ihren „Back-Office-Bereich“ und die Kundenschnittstelle zu rationalisieren.

Der deutsche Bankenmarkt weist einige Besonderheiten auf, z.B. mit dem Zentralen Kreditausschuss (ZKA), einer Vereinigung aus Interessenvertretern der Bankenverbände, der das koordinierte Vorgehen und die Einführung von Innovationen auf breiter Front im Bankgeschäft fördert. Diese Koordination wird von Kritikern als Wettbewerbsbeschränkung und Innovationsbremse durch die Bankenmacht und die Bankenabkommen gesehen. Die dadurch erreichte garantierte, flächendeckende, abgestimmte Einführung neuer Verfahren wird jedoch durchweg als positiv bewertet.

Die Motive der Banken für den Einsatz elektronischer Zahlungssysteme werden durch die nachfolgend beschriebenen Ziele und Interessen beeinflußt:

- Rationalisierungsziele
- Auslastung der bestehenden technischen Infrastruktur
- Kontrollinteresse
- erweiterte Kreditschöpfungsmöglichkeiten
- Gewinne aus Wertstellungsunterschieden

Rationalisierungsziele;
Aus ökonomischen Aspekten ist es für Kreditinstitute sinnvoll, das Zahlungsverkehrsangebot, das auf Buchgeld basiert, auszubauen und zu optimieren, um das Aufkommen an Bargeldgeschäften zu reduzieren.
Zum einen sind die Refinanzierungskosten der Kreditinstitute für Buchgeld deutlich niedriger als für Bargeld. Für einen Hundertmarkschein muß eine in Deutschland ansässige Bank 100,- DM an die Zentralbank bezahlen, während für die Bereitstellung von 100,- DM Buchgeld nur Kosten in Höhe von 10,- DM, für die Hinterlegung der Mindestreserve und der Barreserve von etwa je fünf Prozent entstehen [Luk97]. Hierbei sind die Kosten für spezielle Sicherheitsvorkehrungen im Bargeldgeschäft, wie z.B. Tresore, mit Panzerglas gesicherte Kundenschalter oder Sicherheitstransporte, noch nicht berücksichtigt. Diese Distributionskosten werden nur zum Teil von den Banken getragen, Händler und Verbraucher tragen diese Kosten ebenfalls. Bei der Untersuchung der Wirtschaftlichkeit für die Banken müssen diesen Kosten die Systemkosten für elektronische Zahlungssysteme gegenüber gestellt werden.
Zum anderen sind die Banken daran interessiert, die personal- und deshalb kostenintensive Belegverarbeitung zu reduzieren. Durch eine durchgängige IT-

Unterstützung kann das Belegaufkommen minimiert werden, da eine unmittelbare Weiterleitung der digitalen Transaktionsdaten möglich ist. Die Kostensituation sei an einem Beispiel von Stolpmann verdeutlicht, der die Kostensituation für Online Transaktionen im Vergleich mit der personalintensiven und dadurch teuren Kundenbetreuung in Filialen bewertet: „*So kostet eine Überweisung vom heimischen PC das Kreditinstitut nur 0,15 DM - 1,20 DM. Per Telefon kostet sie schon 2,-- bis 3,-- DM und am Schalter gar 3,-- bis 4,-- DM für die Banken.“* [Stol97, S.84] Er merkt jedoch auch an, daß ein Filialnetz weiterhin bestehen muß, solange es keine Möglichkeit gibt, Ein- und Auszahlungen online vorzunehmen.

Auslastung der bestehenden technischen Infrastruktur;
Die Banken haben ein großes Interesse daran, daß die bestehende Infrastruktur genutzt und integriert werden kann und somit die Rentabilität der, in der Vergangenheit getätigten, Investitionen geschützt ist. Dieser Investitionsschutz ist gleichsam für Kunde und Finanzinstitut ökonomisch wirksam. Die Kunden können ihre *POS-Struktur*[8] weiter nutzen und die Händler können weiterhin die *POS-Kassen* und Kreditkartenlesegeräte für die *POS-Abrechnung* einsetzen. Auch unter dem Gesichtspunkt der vertrauensbildenden Maßnahmen, die einen kritischen Erfolgsfaktor im Kunde-Bank-Verhältnis darstellen, ist das Fortführen der bestehenden Infrastruktur bedeutsam. Von Niehoff wird sogar die Rücknahme der Innovationsgeschwindigkeit in Erwägung gezogen, da ein kritischer Akzeptanzpunkt in der erwarteten Lebensdauer eines Produkts, in diesem Falle Zahlungssysteme, liegt. Muß der Benutzer davon ausgehen, daß der Lebenszyklus des Zahlungssystems sehr kurz ist und das System nur kurze Zeit am Markt verfügbar ist bevor es durch ein neues, meist innovativeres Produkt abgelöst wird, wird dies seine Entscheidung für ein System beeinflussen [Nie98].
„*Die Banken haben trotz der technischen Realisierbarkeit z.B. von Chipkartenlösungen lange keine solchen Systeme eingesetzt bzw. forciert, was teilweise auch auf die hohen Sicherheitsanforderungen für die Schlüssellängen zurückzuführen ist*“ [Nie98], so die Aussage eines Vertreters des Bundesverband Deutscher Banken e.V, Köln. Denkbar ist aber auch, daß man das aufgebaute und noch aufzubauende POS-System nicht in Frage stellen will und deshalb der Einsatz der *GeldKarte* und des *EC-Cash*, im Internet nicht schneller vorangetrieben wird [Rie98].

Kontrollinteresse;
Die Banken und Sparkassenverbände nehmen auf den Standardisierungsprozeß Einfluß. Diese Bestrebungen sind zum einen dadurch motiviert, daß die Kreditinstitute den Anschluß nicht verlieren und den derzeitigen Trend für den Ausbau ihrer Geschäftstätigkeit nutzen wollen, zum anderen soll der Markt gegenüber anderen Konkurrenten durch den Einsatz von hohen Marktzugangsbarrieren gesichert werden. Die Etablierung des *HBCI-Standards* ist ein konkretes Beispiel für diese Einflußnahme. Der Grundstein für den Ausbau der Geschäftstätigkeit wurde schon bei der Definition der standardisierten Geschäftsprozesse für Online Informationen und elektronische

[8] POS (**P**oint **o**f **S**ale)

Transaktionsaufträge[9] gelegt, die die Lenkung der Zahlungsströme über die institutseigenen Servicezentren ermöglichen. Den Banken, als Emittent von digitalen Münzen, eröffnet sich die Chance Kundenbindung über die Verrechnungskonten zu erreichen.

erweiterte Kreditschöpfungsmöglichkeiten;
Im Rahmen der Novellierung des Gesetzes über das Kreditwesen (KWG) wurde die Emission elektronischen Geldes in den Katalog der Bankgeschäfte aufgenommen[10], um damit die Ausgabe elektronischer Zahlungsmittel auf Kreditinstitute zu beschränken. Die Schaffung und Verwaltung von Netzgeld ist Bankgeschäft und unterliegt somit der traditionellen strikten Aufsicht und der Geldmengenregulation durch die Bundeszentralbank - wurde im Vorfeld der vollzogenen Gesetzesänderung argumentiert.
Eine Kernfunktion der Zentralbank - die Sicherung der Währung, durch geldpolitische Maßnahmen - wäre nachhaltig gestört, wenn vermehrt elektronisches Geld in Umlauf gebracht würde, das nicht durch die Zentralbank Mindestreserve abgedeckt ist. Inwieweit diese Steuerungsmaßnahmen auf den digitalen Geldmengenumlauf wirksam werden können, ist fraglich, da durch die weltweite Verbreitung und den dezentralistischen Ansatz des Internets länder- oder gar kontinentalspezifische Regelungen nicht greifen. Die Bundesbank hat deshalb in ihrem Maßnahmenkatalog unter anderem eine Erweiterung der statistischen Meldepflicht und der Mindestreservebasis gefordert. Diese Forderung läuft konträr zur Interessenlage der Banken, da diese sich tendenziell dem geldpolitischen Zugriff der Bundesbank entziehen möchten, um sich dadurch erweiterte Kreditschöpfungsmöglichkeiten zu eröffnen.

Gewinne aus Wertstellungsunterschieden;
Die Begleichung einer Transaktion kann mit digitalem Geld sofort erfolgen, dies könnte zu einer Vereinfachung des komplexen Netzwerks von Verbindlichkeiten und Anleihen führen [Lyn97]. Dies ist nicht unbedingt im Interesse der Kreditinstitute, die mit der Batch-Verarbeitung ihre Valutastellung begründen. Bei einer Wertstellung in Echtzeit würde eine Einnahmequelle der Kreditinstitute wegfallen.

---

[9] In Abgrenzung zu Abholaufträgen, haben Transaktionsaufträge nicht nur einen Informationsfluß, sondern reale Transaktionen zur Folge (z.B. Überweisungsauftrag). [vgl. HBCI98; Kap. II, S. 29]

[10] KWG §1 (1) „*Bankgeschäfte sind ... 12. die Schaffung und die Verwaltung von Zahlungseinheiten in Rechnernetzen (Netzgeldgeschäft)* „ [KWG97].

3.4 Andere Teilnehmer

Neben den beschriebenen Teilnehmern, Händler, Kunde und Banken, sind weitere Interessengruppen involviert, die Motive für den Einsatz von elektronischen Zahlungssystemen haben. Sie alle wollen ein Stück von dem umsatzstarken „Kuchen“ *E-Commerce* abhaben.

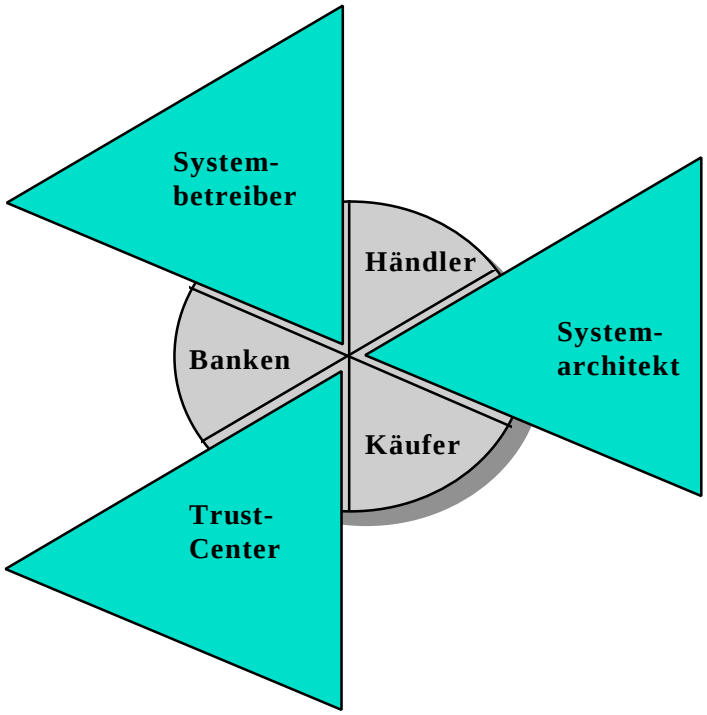


Abbildung 3-4; Interessengruppen elektronischer Zahlungssysteme

Der **Systemarchitekt** entwickelt das Zahlungssystem und prägt den Produktnamen (*branding*) [Schu97]. Er ist für den Update und die Weiterentwicklung des Systems zuständig, die durchgeführt werden, um den wachsenden Anforderungen gerecht zu werden.
Er kann seinen finanziellen Nutzen aus der weiteren Verbreitung seines Brandings ziehen, oder kostenpflichtige Lizenzen an die Systembetreiber vergeben.

Der klassische **Systembetreiber**, ist ein Intermediär zwischen Händler und Banken, der sämtliche Händlereinnahmen an die Banken weiterleitet und das Clearing für den Händler übernimmt. Er berechnet für seine Dienstleistung Gebühren oder ist am Umsatz beteiligt.
Für den reibungslosen Ablauf der Installation und der Wartung des Systems bei Käufer und Händler ist der Systembetreiber verantwortlich.

Trust-Center oder Zertifizierungsstellen haben die Aufgabe, kryptographische Schlüssel für Individuen auszugeben. Diese Form einer zentralen, sicheren und vertrauenswürdigen Infrastruktur ist jedoch nur für einen Teil der elektronischen Zahlungssysteme notwendig.

3.5 Zusammenfassung

Inwieweit die von den **Banken** forcierten Zahlungssysteminnovationen bedarfsgerechte und nachfrageorientierte Lösungen darstellen ist zu hinterfragen. Unstrittig ist jedoch, daß die Banken am Zahlungsgeschäft und dem daraus resultierenden Anschlußgeschäft interessiert sind und schon allein deshalb den Interessen des Kunden und der Kundenbindung gerecht werden.

Die Interessenlage der Banken stellt sich so dar, daß Innovationen, die nicht unter der Kontrolle der Banken stattfinden, Einnahmequellen oder Einsparungspotentiale der Banken schmälern oder den Erfolg bereits bestehender Zahlungssysteme der Kreditwirtschaft in Frage stellen, nicht forciert werden[Rie98].

Im Kontext der Internationalität des Internets und der Liberalisierung stellt eine Politik der Verzögerung oder gar Blockade von Innovationen, wie sie teilweise von deutschen Banken betrieben wird, eine Gratwanderung dar. Der Markteinfluß eines *global Players* könnte, unter bestimmten Voraussetzungen, zu einer Neuordnung des Marktgefüges führen, und somit auch die Position der Banken bedrohen. Zudem haben unter Globalisierungsaspekten deutschlandweite Standards und Bestimmungen im globalen Netz wenig Nutzen, vielmehr gilt es Konzepte neuer elektronischer Zahlungssysteme mitzugestalten.

Das Interesse des **Käufers,** für den Einsatz elektronischer Zahlungssysteme, liegt vorrangig in der Möglichkeit bequem, zeit- und ortsunabhängig einkaufen zu können.

Es wird vorausgesetzt, daß elektronische Zahlungssysteme mindestens die Anforderungen an herkömliche Zahlungssysteme erfüllen. Darüber hinaus soll sich das System in die Prozesskette (*Customer Bying Cycle)* des Käufers einfügen, um deren durchgängige Medienunterstützung sicherzustellen. Der Käufer kann, mittels der Durchgängigkeit der IT-Unterstützung, ein Mehrwertpotential erschließen.

Nur wenn elektronische Zahlungssysteme verfügbar sind, kann die breite Palette des E-Commerce genutzt werden. Besonders unter dem Aspekt der exclusiven Online-Verfügbarkeit von Informationen oder Dienstleistungen bestehen vermehrt Anreize, im Internet elektronisch bezahlen zu können.

An den zukunftsweisenden Technologien und Möglichkeiten der Informationsgesellschaft teilzuhaben ist ein weiteres Motiv, das den Besitz eines Zahlungssystems erstrebenswert macht. Diese Motivation ist aber nicht allen Konsumenten gemein, vielmehr geben die ungelösten Fragen des Technikeinsatzes Anlaß die wahrscheinlichen Auswirkungen der Technologien kritisch zu hinterfragen und individuell zu beurteilen, ob dies erstrebenswert ist.

Der Verkauf und die Bestellmöglichkeit über das Internet eröffnen dem **Händler** ein enormes Kundenpotential. Durch qualifizierte Maßnahmen, wie Profiling und Matching, können Systeme unterstütz werden, die die Bindung dieses Kundenpotentials an den Händler erhöhen und effiziente Marketingstrategien ermöglichen.

Durch die Optimierung der Abläufe von Handelstransaktionen, werden Synergie- und Rationalisierungseffekte genutzt, die sich direkt auf die Kostensituation des Unternehmens auswirken. Außerdem ist, in der Prozesskette des Händlers, ein nicht unwesentliches Unterstützungspotential für elektronische Zahlungssysteme zu identifizieren.

4 Akzeptanzkriterien

Dem Internetnutzer werden heute bereits eine Vielzahl von Zahlungsmöglichkeiten angeboten. Eine Studie von Karl Kurbel und Frank Teuteberg von der Europa-Universität Viadrina in Frankfurt (Oder) im dritten Quartal 1997 ergab [KuTe97], daß nur ein Drittel der Unternehmen in Deutschland das WWW auch für den Verkauf einsetzen (Zweck des WWW ist Verkauf über das Internet 34,8%). Nach Angaben der ausgewerteten Fragebogen setzte sich das Zahlungsmittel-Mix für die Bezahlung der bezogenen Leistungen, die über das Internet angeboten wurden, wie folgt zusammmen:

Zahlungsweise	Angaben in %
Rechnung	52,6
Bankeinzug	25,4
Scheck	17,6
Kreditkarte	16,6
Cybercash	2,7
Andere	12,0

Um Handlungsalternativen aus diesen statistischen Zahlenmaterial ableiten zu können, bzw. die erkennbaren Trends begründen zu können, müssen die Kriterien der Akzeptanz herangezogen werden.

4.1 Sicherheit

Die deutsche Bevölkerung hat ein sehr hohes Sicherheitsbedürfniss. Nach einer Marktuntersuchung der Firma *inTouch* über Cyber Money verlangen 93 Prozent der Bundesbürger hohe Sicherheitsstandards für den Handel im Internet, bevor sie diesen nutzen. [Zeit51'97]

Obwohl kein System bekannt ist, das eine hundertprozentige Sicherheit gewährleisten kann, gibt es die Fiktion von der totalen Sicherheit immer noch. Die Diskrepanz zwischen dem hohen Sicherheitsbedürfniss und der „meßbaren" Sicherheit eines Systems, anhand des Systemverhaltens bei Gefahr, ist gegeben. Um die Gefahren einschätzen zu können, bedarf es Informationen, die es erlauben, ein Bewußtsein für das Risiko zu entwickeln. In naher Zukunft wird mehr Risiko auf uns zukommen, das wir tragen müssen [Her98]. Dies ist vorallem durch die Vielfalt der Informationen, die das Risikobewußtsein erst schaffen, bedingt. Zudem entstehen rechtsfreie oder vermindert, durch etablierte Gesetze, geregelte „Räume". Es wird ein **Gefühl von Sicherheit** entstehen, durch die Qualifikation und Quantifizierung des Risikos.

Man ist bestrebt, die Sicherheit eines Systems möglichst nahe an die Hundertprozent-Marke anzunähern und die bestehende Gefahr in Risiko zu wandeln. Dieser Wandel vollzieht sich durch das Erkennen von potentiellen Gefahren oder Schwachstellen des Systems und der Bewertung möglicher Schadensfälle bzw. der Ableitung von Handlungsalternativen. Bei der Bewertung wird der Koeffizient der Sicherheitsrentabilität betrachtet.

Sicherheitsrentabilität ist eine Investitionskenngröße, die den möglichen Aufwand durch kriminelle Manipulation (Verluste durch Manipulation, Opportunitätskosten durch Imageschäden und Aufwendungen zur Schadensbehebung) eines Systems den mit dem System verbundenen Schutzaufwendungen (Initialkosten und Folgekosten durch Betrieb, Logistik, Service, Updates) gegenüberstellt. [Stol97, S. 91]

Softwarebasierte Lösungen schneiden bei diesem Vergleich meist besser ab als Hardwarebasierte, obwohl letztere per se ein höheres Sicherheitspotential bergen.

4.1.1 IT-Sicherheit

Sicherheit ist kein Selbstzweck. Die IT-Sicherheit muß als dienende Funktion eingesetzt werden, um die Schutzanforderungen der Akteure zu befriedigen [Büll98]. Aus den Schutzanforderungen der Teilnehmer abgeleitet definiert Pfeffer die „Grundsätze der Sicherheit“ und die IT-Maßnahmen, die zur Realisierung eingesetzt werden wie folgt [Pfeff96]:

Grundsatz der Sicherheit	**IT-Maßnahme**
Vertraulichkeit Kein unbefugter Dritter darf Zugriff auf die ausgetauschten Informationen haben.	**Verschlüsselung** asymmetrisch: RSA, Diffie-Hellmann, ElGamal symmetrisch: IDEA, DES
Integrität Daten, die in einer Transaktion verwendet werden, dürfen während der Übermittlung nicht verändert werden. Die gesendeten Daten müssen mit den empfangenen Daten übereinstimmen.	**Hash-Funktionen,** **Message Digest,** **Message Authentication Code**, (MD5, SHA)

Grundsatz der Sicherheit	**IT-Maßnahme**
Authentizität Es muß sichergestellt sein, daß alle Teilnehmer an einer Transaktion auch diejenigen sind, für die sie sich ausgeben.	**Übertragungsprotokolle, Kerberos**, *zur Authentifizierung der kommunizierenden Computer* **Paßwort, Digitale Signatur, Biometrik, Smartcard,** *zur Authentifizierung des Anwenders*
Protektion von Teilen der Information Die verschiedenen Beteiligten an einer Transaktion haben ein unterschiedliche Informationsbedürfnisse. Damit jeder Beteiligte nur die für ihn relevanten Daten lesen kann, muß die Möglichkeit bestehen nur Teilbereiche der Transaktion (z.B. die Bestellinfo) zugänglich zu machen.	**digitaler Umschlag** **blind Signature**
Verbindlichkeit Die übermittelten Informationen und Willenserklärungen müssen verbindlich und im Streitfall nachweisbar bzw. nicht abstreitbar sein.	**digitale Signaturen** **Schutz vor replay attack durch Zeitstempel**

4.1.2 Mehrseitige Sicherheit

Lutterbeck vertritt die These: „Die Sicherheit eines Zahlungssystems ist - auch - abhängig von dem ökonomischnen Modell, das sicher gemacht werden soll.“ [Lut98]

Der Begriff Sicherheit im Kontext der elektronischen Zahlungssysteme geht weit über den Definitionsrahmen der klassischen IT-Sicherheit hinaus. Die technischen Sicherheitsvorkehrungen sind als Basis für eine „mehrseitige Sicherheit“ anzusehen, die verschiedenste Anwendungsszenarien in ihre Betrachtung miteinschließt. Die mehrseitige Sicherheit ist um die Dimensionen technisch-organisatorisch, rechtlich-ökonomisch und gesellschaftlich erweitert.

Im Bereich der **gesellschaftlichen** Rahmenbedingungen sind sicherheitsrelevante Fragen im Bezug auf systemische Risiken, informationeller Selbstbestimmung oder die Auswirkungen auf die Arbeitswelt zu beantworten.

Der **rechtlich-ökonomische** Aspekt beschäftigt sich mit der Einführung bzw. Umsetzung von Gesetzen und Verordnungen, Fragen des Verbraucherschutzes oder Haftungsfragen. Juristen stehen vor gewaltigen Problemen, bei der juristischen Absicherung von Vertragsabschlüssen und Zahlungen im Internet. Die wichtigsten rechtsfreien Bereiche sind nach [Bön95]:

- Schutz des Eigentums
- Zuständigkeit und Verantwortlichkeit für Inhalte
- Haftung der Internet-Dienste-Anbieter

Die **technisch-organisatorische** Dimension berücksichtigt Sicherheitsaspekte durch die Einführung von Standards. [Zoch98]

4.1.3 Vertrauen

Ein sicheres, fehlertolerantes System schafft Vertrauen, Vertrauen in die Technologie durch die IT-Sicherheitsmaßnahmen und Vertauen in die rechtliche und gesellschaftliche Vertretbarkeit durch die mehrseitige Sicherheit. Die Frage nach der Vertrauenswürdigkeit des Vertrags- bzw. Kommunikations-Partners ist der dritte Aspekt zum Thema Sicherheit.

Um Vertrauen zu schaffen braucht es mehr als nur Verfahrensweisen zur Sicherstellung von Zahlungen. Möglichkeiten zur Prüfung von Referenzen und Leumund, sowie zur Erlangung des zu letzt genannten, werden gefordert [Lyn97].

Im Internet ist per se keine Vertrauensinstanz vorhanden, Geschäfte werden im guten Glauben oder in der Hoffnung, die Ware bzw. das Geld zu erhalten, abgewickelt. Dies gilt für Erstkontakte, nicht jedoch für Kunden, die wiederholt in Geschäftebeziehungen mit dem Anbieter stehen, da hier auf die Erfahrungswerte als **Vertrauensbasis** zurückgegriffen werden kann. Bei diesem Modell des Vertrauensnetzwerks müßte jeder Käufer mit jedem Händler eine Vertrauensbeziehung etablieren.

Es besteht jedoch die Möglichkeit Vertrauensbeziehungen außerhalb des Netzwerks zu nutzen, wie die der Banken, Notare etc. Durch das Hinzuziehen von **vertrauenswürdigen Dritten** kann eine Infrastruktur des Vertrauens aufgebaut werden, an der Käufer und Händler gleichermaßen partizipieren können. Grundsätzlich werden zwei Ansätze zur Realisierung dieser Infrastruktur unterschieden: Der zentrale Ansatz, mit einer univalenten Instanz (z.B. W3 trusted WebPages) oder einer „Root-Instanz“ in Hierarchien (z.B. Zertifizierungsmanagement), und der dezentrale Ansatz, der aus einem Netzwerk von einander vertrauender Individuen besteht (z.B. PGP[11]), die als Vertrauensmittler fungieren [Cav95].

[11] PGP (**P**retty **G**ood **P**rivacy): E-Mail-Verfahren, das durch die Weitergabe von öffentlichen Schlüsseln der Benutzer, almählich ein Netzwerk des Vertrauens bildet.

Inwieweit Sicherheit aus Vertrauen transitiv ist, wie das im zuletzt dargelegten Ansatz vorausgesetzt wird, ist fraglich [Wic98].

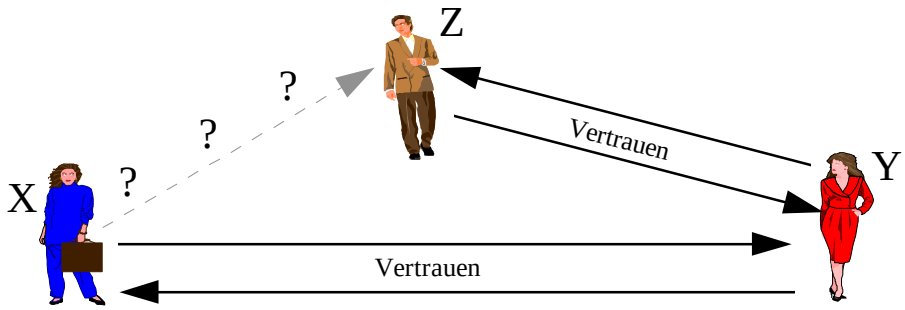


Abbildung 4-1; Sicherheit aus Vertrauen

Es kann sein, daß Teilnehmer X dem Teilnehmer Z vertraut, weil X dem Teilnehmer Y vertraut und Z für Y vertrauenswürdig ist, es muß aber nicht zwangsläufig so sein.

4.2 Anonymität und Datenschutz

Das Recht auf Datenschutz und Anonymität stellt im modernen Rechtssystem ein Grundrecht dar. Verbraucherverbände fordern die Umsetzung dieses Rechts durch ein Minimieren des „Sammeln“ von persönlichen Daten.

Kollmann definiert die **verbraucherpolitischen Ziele** wie folgt: [Kol98]

- Die Datengenerierung selbst ist zu minimieren.
- Daten von Verbrauchern haben in deren Einfluß- und Korrekturbereich zu verbleiben.
- Gesamtgesellschaftlich optimale und transparente Lösungen mit brauchbaren Konfliktlösungsmechanismen sind zu entwickeln.
- Systembetreiber haben Systemrisiken zu tragen und nicht die Verbraucher.

Es bedarf Alternativen, die es dem Käufer ermöglichen, seine persönlichen Daten und deren Speicherung, auf Grund transparenter Informationen welche Daten für wie lange, wo gespeichert werden, zu kontrollieren, oder aber völlig anonym zu bleiben. Mit der Benutzung eines Zahlungssystems darf nicht zwingend das Einverständnis zur Erstellung von Benutzerprofilen gefordert werden, die es ermöglichen Mehrwerte zu generieren, wie z.B. Marketingaktionen gezielter anzusetzen.

Der Versuch ein digitales Gegenstück zum Bargeld zu schaffen, das dessen Vorteile, nicht jedoch dessen Nachteile in sich vereinigt, gestaltet sich schwierig. Untersucht man

die Beweggründe für das Bezahlen mit Bargeld, so ist die gewährleistete Anonymität und die daraus resultierende Wahrung der Privatsphäre ein Hauptkriterium. Ein Zahlungssystem ohne Anonymität und Datensparsamkeit wird keine weite Akzeptanz finden. [Pfi98]

Als ein kritisches Akzeptanzkriterium sieht Peter Zoche den Datenschutz und die Datensicherheit in seinem Thesenpapier „... Wenn eine weite Akzeptanz der neuen Zahlungssysteme erreicht werden soll, muß Datenschutz und Datensicherheit verstärkt als Element einer erhöhten Dienstleistungsqualität aufgefaßt und als integraler Angebotsbestandteil angesehen werden.“ [Zoch98]

4.3 Komplexität

Der Grad der Komplexität kann durch eine gezielte nutzeradäquate Informationsgestaltung und software-ergonomisch gestaltete Nutzerschnittstellen verringert werden. Bei der Informationsgestaltung müssen die verschiedenen Akteursgruppen wie z.B. Händler, Käufer, etc. berücksichtigt werden. Durch eine spezifische Didaktik, die das medienkompetente Handeln unterstützt und auf die individuellen Bedürfnisse der Akteursgruppen zugeschnitten ist, wird der intellektuelle Zugang zum System erleichtert.

Bei einer Umfrage von Weiler 1996 wurde von Internetnutzern die ***Einfachheit in der Benutzung*** an erster Stelle in der Rangfolge genannt. Gefolgt von Übertragbarkeit, Sicherheit und Interoperabilität als weitere bedeutsame Eigenschaften von Geld im Internet [Vah97].

Um die Nutzerakzeptanz zu erhöhen, sollten für den Anwender aufbereitete Informationen, über die technische Funktionen und deren Handhabung, Systemvoraussetzungen, Zugangsmöglichkeiten zum System, Sicherheitsaspekte des Systems und Hinweise auf rechtliche Konsequenzen und andere Besonderheiten, zur Verfügung gestellt werden [Zoch98].

4.4 Zusammenfassung

Technische Verfahren, mit dem Ziel die IT-Sicherheit zu erhöhen, sind in einer Vielzahl entwickelt worden. Da sich beim *Online-Bezahlen* der Sicherheitsaspekt über die technische Sicherheit hinaus erstreckt, reichen diese Methoden nicht aus, um das Sicherheitsbedürfnis des Benutzers zu befriedigen. Mehrseitige Sicherheit und vertrauenssichernde Maßnahmen für die Handelstransaktionen werden gefordert. Deren Entwicklung und Umsetzung ist jedoch noch nicht weit genug fortgeschritten bzw. etabliert, um von einer zufriedenstellenden Situation sprechen zu können.

Die Entscheidung, wieviel Anonymität bei der Transaktionsabwicklung gewahrt werden soll, sollte dem Benutzer überlassen werden. Entscheidungsvoraussetzung ist die möglichst umfassende Information des Benutzer, die eine „*Kultur des Mißtrauens*“ [Ulr98] durch Aufklärung ermöglicht.

5 Ableitung der kritischen Erfolgsfaktoren

Die Erfolgsfaktoren werden aus den Motivationsgründen für elektronische Zahlungssysteme (vgl. Kap. 3) und den Akzeptanzkriterien (vgl. Kap 4) abgeleitet. Sie dienen als **Bewertungsmaßstab** für die in den folgenden Kapiteln dargelegten Konzepte.

Die Einteilung der kritischen Erfolgsfaktoren erfolgt in zwei Kategorien Initial- und Treuekriterien [vgl. Pern97, S.346]

- **Initialkriterien:**
  - allgemeine Verbreitung
  - Durchgängigkeit der IT-Mittel
  - technische Integrationsfähigkeit
  - Anwendungsintegration
  - Unterstützung grenzüberschreitenden Zahlungsverkehrs
  - Ergonomie
  - Effizienz
  - Skalierbarkeit
  - geringer Kostenaufwand
  - Zahlungszeitpunkt

- **Treuekriterien**:
  - Verlusttoleranz
  - Fairer Handel
  - Datenschutz / Anonymität
  - Sicherheit
  - Verfügbarkeit und Zuverlässigkeit

5.1 Initialkriterien

Unter dem Begriff Initialkriterien werden all diejenigen Kriterien zusammengefaßt, die bei der ersten Auswahl eines Zahlungssystems in die Bewertung miteinfließen.

- **allgemeine Verbreitung**

Eine große Anzahl von Händlern und Kunden sollten das System einsetzen, damit ein möglichst großes Einsatzspektrum gewährleistet ist. Über die Akzeptanz und Verbreitung eines Zahlungssystems entscheiden jedoch nicht nur fachliche Kriterien, sondern auch Imagewerte, Publicity und andere Einflußfaktoren.

- **Durchgängigkeit der IT-Mittel**

Um eine durchgängige Unterstützung ohne Medienbruch zu realisieren müssen alle eingesetzten IT-Mittel innerhalb eines Mediums verfügbar sein. Zum Beispiel sollten alle Funktionalitäten des Zahlungssystems über Internet-Technologien handhabbar sein, von der Initialisierung des Zahlungssystems über den Geldtransfer bis hin zur Abmeldung oder der Rückgabe des Zahlungssystems.

- **technische Integrationsfähigkeit**

Realisierung von definierten, offengelegten Schnittstellen, unter Berücksichtigung der speziellen Anforderungen der Portabilität und Systemunabhängigkeit.
Es sollte keine zusätzliche Hardware wie z.B. neue Lesegeräte am POS erforderlich sein. Vielmehr ist ein erklärtes Ziel, der Rückgriff auf die verbreitete Infrastruktur mit bewährter Technologie.

- **Anwendungsintegration**

Die Zahlungssystem-Applikation greift auf definierte Formate und für den Einsatz im Internet optimierte, redesignte Geschäftsprozesse zurück. Der durchgängige Informationsfluß ist hierüber sichergestellt.

- **Unterstützung grenzüberschreitenden Zahlungsverkehrs**

Zahlungssysteme die grenzüberschreitend effizient eingesetzt werden können, sind unter Berücksichtigung der zunehmenden Globalisierung der Märkte erforderlich.

- **Ergonomie**

Es wird Wert auf die intuitive Bedienbarkeit des Systems gelegt. Die Argumente für die Sicherheit des Systems sollten einfach strukturiert und leicht verständlich sein.

- **Effizienz**

Vor allem die technische Unterstützung des Zahlungssystems ist hier als kritischer Faktor zu sehen. Lange Wartezeiten beim Kommunikationsaufbau und komplizierte, formale, bürokratische Abläufe sind hinderlich. Es ist zu berücksichtigen, daß abhängig vom Werteumfang Kleinsttransaktionen andere Mechanismen verlangen als „Millionengeschäfte“.

- **Skalierbarkeit**

Die technischen Kapazitäten des Systems sollten mit steigender Teilnehmerzahl auch erweitert werden können, so daß kein überproportionaler Leistungsverlust bei Vollauslastung entsteht.

- **geringer Kostenaufwand**

Diesem Kriterium der Kosten/Nutzen-Analyse muß eine hohe Priorität eingeräumt werden, da die Kosten darüber entscheiden, ob und in welchem Ausmaß ein Zahlungssystem wirtschaftlich sinnvoll eingesetzt werden kann.

- **Zahlungszeitpunkt**

Der Zeitpunkt der Belastung des Kontos (pre-paid / post-paid) wird bei der Auswahl eines Zahlungssystems ebenfalls bewertet.

5.2 Treuekriterien

Die Treuekriterien beschäftigen sich mit den Argumenten für das weiter andauernde Benutzen eines Zahlungssystems, für das man sich irgendwann einmal entschieden hat. Somit stellen Treuekriterien die Hemmschwelle für den Wechsel zu einem anderen Zahlungssystem dar.

- **Verlusttoleranz**

Daten in einem Zahlungssystem, die monetäre Werte repräsentieren, sind besonders schützenswert. Für den Benutzer ist es wichtig, Möglichkeiten angeboten zu bekommen, sich vor unverschuldetem Verlust zu schützen, bzw. die Werte nach deren Zerstörung rekonstruieren zu können.

- **Fairer Handel**

Auf Dauer kann kein System erfolgreich agieren und Kunden binden, wenn die Gestaltung von rechtlichen Grundlagen wie Haftungsrisiko etc. nicht beiden Geschäftsparteien gerecht wird.

- **Datenschutz / Anonymität**

Der Benutzer muß die Wahlmöglichkeit haben, bei seinen elektronisch abgewickelten Geschäften anonym zu bleiben.

- **Sicherheit**

Für Pernul und Röhm spielt die Sicherheit als Treuekriterium die Hauptrolle [Pern97]. Sie gehen davon aus, daß viele Benutzer von einem Zahlungssystem Abstand nehmen würden, sollten im Betrieb Sicherheitsprobleme auftreten .

- **Verfügbarkeit und Zuverlässigkeit**

Die Zuverlässigkeit und Verfügbarkeit des Systems im laufenden Betrieb, hinsichtlich Netzwerk, Durchsatzgeschwindigkeit, Hard- und Software, muß gewährleistet sein.

6 Ausgewählte Elektronische Zahlungssysteme im Internet

In diesem Kapitel werden elektronischen Zahlungssysteme betrachtet, deren Entwicklungsfortschritt über eine Pilotimplementierung hinausgeht. Die Einschränkung, daß die Systeme im Internet einsetzbar sein müssen, filtert elektronische Zahlungssysteme, deren eingesetzte Methoden in einem multinationalen Kontext zur Verfügung stehen und nicht durch gesetzliche Regelungen oder Exportbeschränkungen blockiert sind [OII97]. Eine weitere Einschränkung erfolgt durch die Maßgabe, daß vorrangig Systeme, die im Bereich Business-to-Consumer eingesetzt werden, untersucht werden.

Es werden zunächst Protokolle für Zahlungstransaktionen näher erläutert, die Basis für dedizierte Zahlungsmittel sind. Die dann folgende Beschreibung der Zahlungsmittel wird in die Bereiche Micropayments, münz-, kreditkarten- und scheckbasierte Anwendungen unterteilt. Das CyberCash-System und E-Commerce-Frameworks werden in den letzten beiden Abschnitten thematisiert.

Auf Chipkarten basierende Systeme werden in dieser Arbeit, die sich auf Softwarelösungen konzentriert, nicht gesondert aufgeführt. Eine Evaluation[12] der über 20 unterschiedlichen „elektronischen Geldbörsen“ allein in Europa, würde den Rahmen dieser Arbeit sprengen. Auf die GeldKarte des *Zentralen Kreditausschuß (ZKA)* wird im Rahmen des HBCI-Protokolls (vgl. Kap. 6.1.1) eingegangen.

6.1 Protokolle

„Ein Protokoll ist ein ... In der digitalen Kommunikationstechnik ... zumeist standardisiertes Verfahren zur Steuerung von Abläufen zwischen verschiedenen Endgeräten. Damit die Verbindung zwischen Endgeräten und die Kommunikation darüber abgewickelt werden kann, müssen sie dasselbe Protokoll verwenden“ [Siet97, S.182]

In den nachfolgenden Abschnitten werden Protokolle für Zahlungstransaktionen, deren Spezifikation veröffentlicht wurde, näher erläutert.

6.1.1 Homebanking Computer Interface (HBCI)

In Zusammenarbeit mit deutschen Banken, der Sparkassenorganisation und Verbänden hat der Zentrale Kreditausschuß (ZKA) das HBCI spezifiziert. Die veröffentlichte Schnittstellenspezifikation beschreibt eine automatisiert nutzbare, **multibankfähige Homebanking-Schnittstelle**. Die Spezifikation wurde zur Implementation in Kunden- und Kredit-

[12] Smart Euro Initiative ein von der Financial Issues Working Group (FIWG) lanciertes Pilotprojekt, mit dem Ziel die Interoperabilität elektronischer „purses“ grenzüberschreitend zu demonstrieren. http://www.ispo.cece.be/fiwg

institutssysteme freigegeben, und ist in der aktuelle Version 2.0.1 vom 2.2.1998 verfügbar [HBCI98].

Die Vertragspartner des HBCI-Abkommens verpflichten sich, daß jedes Kreditinstitut, das einem Kunden den Datenaustausch im Rahmen des Homebanking ermöglichen will, eine HBCI konforme Schnittstelle anbietet [HBCI97].

> Inwieweit sich der auf deutsche Vertragsparteien beschränkte Standardisierungsprozess auch im **internationalen Umfeld** des Internets etablieren kann, wird die Zukunft zeigen. Bestrebungen, in global ausgerichteten Projekten und Standardisierungskonsortien mitzuarbeiten, sind vorhanden (vgl. Kap. 6.4.2).

Der erarbeitete Schnittstellenstandard HBCI wird das Homebanking nun auch in offenen Netzen wie dem Internet ermöglichen und von T-Online unabhängig machen. Somit ist zumindest von der Netzseite her ein globaler Ansatz möglich. Außerdem wird das umständliche und antiquierte Sicherheitssystem, bestehend aus persönlicher Identifikationsnummer (PIN) und der Transaktionsnummer (TAN), durch zeitgemäße Verschlüsselungs- und Authentifizierungsmethoden [Siet97], der digitalen Kundensignatur abgelöst.

Spezifiziert wird die Schnittstelle zwischen Kundenprodukt und Kreditinstitutssystem. Eine zusätzliche Beschreibung der Schnittstelle zwischen Kundenprodukt und Sicherheitsmedium ist erforderlich, um die Multibankfähigkeit zu gewährleisten. Daher findet sich in den Anlagen zur HBCI-Spezifikation auch eine Spezifikation der Schnittstelle zwischen einem HBCI-Kundenprodukt und einer ZKA-Chipkarte.

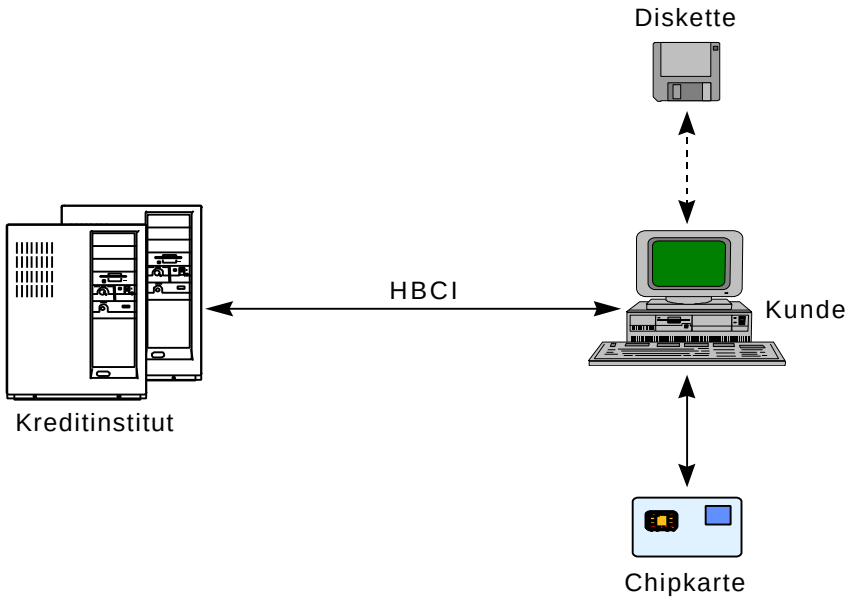


Abbildung 6-1; HBCI Schnittstelle [HBCI98]

Bei HBCI ist keine Verschlüsselungstechnik zwingend vorgeschrieben. Es werden sowohl symmetrische als auch asymmetrische Methoden akzeptiert. Jedes Kreditinstitut hat die Möglichkeit, in seinen *Bankparameterdaten* die unterstützten

Sicherheitsverfahren, d.h. Signatur- und Verschlüsselungsalgorithmen, anzugeben. HBCI definiert nur die **Abfolge der Operationen**. Bei der Erstellung einer Nachricht sind die Arbeitsschritte in folgender Reihenfolge auszuführen (Arbeitsschritte teils optional) [HBCI98]:

1. *Zusammenstellung der Informationen im System des Senders*.
2. *Aufbau der Nachricht*. Aus den Informationen werden die zu übertragenden Segmente bis auf ggf. erforderliche Signatur-Segmente aufgebaut, wobei beim Einstellen der Informationen in die Nachricht Syntaxzeichen entwertet werden.
3. *Bildung der elektronischen Signatur* (optional):
    - Erstellung des Signaturkopfes
    - Berechnung der elektronischen Signatur über Signaturkopf und Auftragssegmente
    - Erstellung des Signaturabschlusses und Einstellung der Daten in das entsprechende Feld
4. *Wiederholung von Schritt 3 für weitere Signaturen* (optional)
5. *Komprimierung* (z. Zt. noch nicht zugelassen)
6. *Verschlüsselung*

Für die Zukunft wird eine **Verquickung** von Electronic Cash und Homebanking angestrebt.

Ein Indiz hierfür ist die geplante Spezifikationsergänzung um den Geschäftsvorfall „Laden der elektronischen Geldbörse“. Über die zeitliche Gestaltung der Erweiterung des HBCI-Standards gibt es jedoch keine konkreten Aussagen. „*HBCI wird schrittweise um weitere Geschäftsvorfälle ergänzt werden. Für die nächste Version sind z.Zt. unter anderem folgende **Geschäftsvorfälle** geplant“ [HBCI98; Kap. I S. 2]:*

- *Wertpapierorder*
- *Abruf von Börsenkursen*
- *Abruf von Einzelumsätzen*
- *Auslandsüberweisung ohne Meldeteil*
- *Laden der elektronischen Geldbörse*

Zum jetzigen Zeitpunkt deckt das HBCI-Protokoll lediglich einen kleinen Ausschnitt der Geschäftsvorfälle aus dem Geldtransferprozess ab, wie z.B. das Erteilen des Überweisungsauftrags auf elektronischem Weg. Würde man diese Funktionalität in die Prozesskette des E-Commerce eingliedern, so könnte für den Händler ein Vorteil darin bestehen, daß der Überweisungsauftrag vom Käufer sofort online angestoßen werden

kann, und so Liegezeiten der Rechnung bis zur tatsächlichen Überweisung des Rechnungsbetrages beim Kunden verringert werden. Ist die Überweisung bei der Bank eingegangen, so sind ab diesem Zeitpunkt keine Valutavorteile für den Zahlungsempfänger, gegenüber der herkömmlichen Abwicklung gegeben, da der Auftrag im Innerbankverkehr noch in der selben Weise erfolgt. Es erfolgt keine Synchronisierung der Wertstellung[13].

> Das HBCI-Protokoll wird, durch die Forcierung über die Kontroll- und Regelementierungseinflüße des ZKA, zumindest auf dem deutschen Markt, einen nicht unwesentlichen Einfluß auf die zukünftigen Software-Entwicklungen nehmen.

Es soll an dieser Stelle noch einmal darauf hingewiesen werden, daß HBCI **kein internationaler Standard** ist, und die zukünftigen Entwicklungschancen, unter dem Aspekt der Globalisierung, kritisch einzuschätzen sind.

6.1.2 i-Key Protocol

IBM's i-Key Protocol (iKP) ist ein sicheres Zahlungsprotokoll, auf der Basis von public-key-Kryptographie und umspannt die Protokolle 1KP, 2KP und 3KP, wobei die Ziffern die Zahl der Parteien angibt, die ihr eigenes Schlüsselpaar besitzen. Der Grad der Sicherheit steigt mit der Anzahl der Schlüsselinhaberparteien und iKP ist so konzipiert, daß aufbauend auf 1KP die weiteren Stufen nachgerüstet werden können. Das iKP ist kein Shopping-Protokoll, es beschränkt sich auf den Geschäftsprozess des *Bezahlens*, d. h. Bestellinformationen werden nicht verschlüsselt oder verifiziert. Grundsätzlich können **sieben Schritte** bei der Abarbeitung einer online Transaktion unterschieden werden, deren Dateninhalte sich von 1KP zu den höheren Protokollen unterscheidet.

1. *Initiierung*: der Käufer initiiert den Protokollfluß
2. *Rechnung*: der Händler antwortet, indem er eine Rechnung an den Käufer sendet
3. *Zahlung*: der Käufer generiert eine Zahlungsanweisung und schickt diese an den Händler
4. *Abbruch*: der Händler hat an dieser Stelle die Möglichkeit das Geschäft abzubrechen
5. *Autorisierungsanfrage*: der Händler schickt eine Autorisierungsanfrage an den Acquirer
6. *Autorisierungsantwort*: der Acquirer nutzt das bestehende Clearingsystem, um die Autorisierung zu erhalten und bestätigt diese dem Händler
7. *Bestätigung*: der Händler leitet die signierte Antwort des Acquirer an den Käufer weiter, zusammen mit anderen zusätzlichen Parametern

[13] Transaktionen mit der GeldKarte sind hiervon ausgenommen.

Das **1KP** ist ein einfaches, effizientes elektronisches Zahlungsprotokoll für offene Netzwerke wie das Internet. Es kommt mit einem **Minimum an Anforderungen** für Zertifizierung, Infrastruktur und dergleichen aus. Nur die Abrechnungsstelle ist in eine Zertifikatsinfrastruktur eingebunden.

Seine **Schwachstellen** sind:

- die Authentifizierung des Käufers erfolgt nur über die Kreditkartennummer evtl. in Verbindung mit einer PIN, ohne die Möglichkeiten der digitalen Signatur auszuschöpfen
- der Händler muß sich weder dem Kunden noch dem Acquirer gegenüber authentifizieren
- weder der Händler noch der Käufer verfügen über einen verbindlichen Auftrag

Das **2KP** verlangt zusätzlich zum Zertifikat des Acquirer, die Zertifizierung des Händlers. Es erfüllt alle Anforderungen von 1KP und zusätzlich:

- Käufer und Abrechnungsstelle gegenüber kann die Authentizität des Händlers, durch dessen Signatur und Zertifikat, nachgewiesen werden.
- der Käufer erhält eine Bestätigung der Transaktion, die sicherstellt, daß der Händler die Zahlung akzeptiert und erhalten hat.

Im **3KP** sind alle Parteien im Besitz eines Schlüsselpaares und korrespondierender Zertifikate. Dies stellt die höchste Sicherheitsstufe dar, mit der Nichtabstreitbarkeit aller verschickten Datenpakete.

> iKP wird mit größter Wahrscheinlichkeit kein großes Marktpotential erreichen, da iKP in die SET-Standardisierung (vgl. Kap. 6.1.3) miteingebracht wurde und die Entwicklungen von IBM nicht weiter forciert wird.

6.1.3 Secure Electronic Transaction (SET)

SET entstand aus den beiden Standardisierungsbestrebungen *Secure Electronic Payment Protokoll (SEPP)* mit *Mastercard*, *IBM*, *Netscape*, etc. *und Secure Transaction Technology (STT)* mit *Visa* und *Microsoft*, die sich im Januar 1996 für eine gemeinsame Entwicklung des SET-Standards entschieden. Diese hinter SET stehende breite Allianz aus namhaften starken Partnern im Finanzdienstleistungsmarkt läßt vermuten, daß **SET zum De-Facto-Standard für Kreditkartentransaktionen im Internet wird**. 1999 soll die „kritische Masse“ erreicht sein für die weltweite Marktdurchdringung des SET-Standards [HerzS98].

> SET baut darauf auf, daß die Karten- und Abrechnungsgesellschaften eine umfassende **Infrastruktur** zur sicheren Zahlungsautorisierung und -abwicklung zur Verfügung stellen.

Die Entwicklungen und Standardisierungsprozesse sind noch nicht abgeschlossen, so daß es sich zum jetzigen Zeitpunkt um einen Zwischenstandard handelt, der immer wieder Änderungen erfährt. Das SET-Protokoll beschränkt sich auf die Definition des

Zahlungsprotokolls, Zusatzkomponenten aus dem Bereich *E-Commerce* werden primär nicht berücksichtigt.

Über ein sogenanntes Zahlungsgateway wird die Schnittstelle zu dieser Infrastruktur definiert. Dieses Zahlungsgateway kann sowohl von einem Acquirer, als auch gemeinsam genutzt von einem Zusammenschluß von Acquirern oder von der Kartengesellschaft selbst betrieben werden. Das Zahlungsgateway stellt das *front end* zu der bestehenden Abrechnungsinfrastruktur dar.

Auf Grund der unterschiedlichen Teilnehmer setzen sich die **Kosten** einer SET-Transaktion zusammen aus den Kosten, die:

- der Acquirer[14] neben dem üblichen Disagio,
- der Betreiber des *Gateways* (kann auch der Acquirer sein),
- der Netz-, Mall- oder Shopbetreiber,
- der Händler

erhebt.

Das SET-Trustmodell baut auf einer **Zertifizierungshirarchie** mit X.509-Zertifikaten auf, die eine Identifizierung der Marktpartner erlaubt, um die übliche Zahlungsgarantie bei Kreditkarten zu gewährleisten. Weder Name des Karteninhabers noch die Kartennummer sind im Zertifikat gespeichert, sondern ein Wert der durch verschiedene Berechnungen und Zufallszahlen generiert wurde. Diese Korrespondenznummer ist mit einer beglaubigten Unterschrift vergleichbar [Pfef96], die von der kartenausgebenden Instanz gespeichert und bei einer Autorisierungsanfrage geprüft wird [O'Mah97].

Eine Aussage über die absolute Höhe der Kosten kann nicht gemacht werden. In welchem Umfang die Beteiligten ihre Betriebs- und zum Teil recht hohen Investitionskosten auf eine SET-Transaktion umlegen können, wird der Markt regeln.

> Das, zunächst auf die Abwicklung von kreditkartenbasierten Transaktionen spezialisierte, SET-Protokoll wird ständig um Funktionalitäten erweitert. Es kann davon ausgegangen werden, daß in naher Zukunft das, von den Initiatoren als offizieller Standard erklärte, SET-Protokoll den Markt noch mehr dominieren wird. Diese Erwartungshaltung ist nicht zuletzt begründet durch die mächtige strategische Allianz, die hinter SET steht.

[14] vertragsunternehmensabrechnende Bank, „acquirer - a bank which collects from merchants the transactions that are submitted to the interchange system and which pays the respective amounts to the merchants on the basis of a merchant agreement" [EwWa93]

6.2 Zahlungsmittel

In diesem Kapitel werden die betrachteten Zahlungsmittel in die Kategorien münzbasierte, kreditkartenbasierte, scheckbasierte Systeme und Micropayments untergliedert. Bei den Zahlungsmitteln handelt es sich im Vergleich zu den Zahlungsprotokollen um konkrete Anwendungen, die vom Endbenutzer eingesetzt werden können.

6.2.1 Münzbasierte Systeme

Lynch definiert digitales Geld als „...elektronischer Ersatz für Bargeld...“ [Lyn97].

Dem entsprechend sind auch die Vorteile des digitalen Geldes denen des Bargeldes ähnlich. Vorteile wie z.B. die sofortige Verfügbarkeit, die besonders für kleine Händler, für die es schwierig ist, die Zeit zwischen dem Verkauf der Ware und dem Erhalt des Geldes zu finanzieren, ein wichtiges Kriterium ist [vgl. Abschnitt 3.1]. Für die Konsumenten ist der Aspekt der optionalen Anonymität und des Datenschutzes als wichtige Eigenschaft der elektronischen Münzen hervor zu heben.

Die Bank für Internationalen Zahlungsausgleich (BIZ) definiert elektronisches Geld als „...ein vorausbezahltes Geldprodukt, das auf einem elektronischen Endgerät gehalten wird, das sich im Besitz des Konsumenten befindet...“.

Diese Definition stellt den Unterschied von elektronischem Geld zu Hard- und Softwareprodukten heraus, die elektronische Kommunikationskanäle wie das Internet lediglich als Gateway zu den herkömmlichen Zahlungssystemen, wie z. B. dem Kreditkartenabrechnungssystem, nutzen.

Bartmann und Fortschki unterteilen das elektronische Geld zusätzlich in **Netzgeld** und **elektronische Geldbörsensysteme** [Bar97]. Die bisher realisierten Formen von digitalen Geld sind bargeldäquivalent, jedoch keine Bargeldsurrogate, da die Eigenschaft des gesetzlichen Zahlungsmittels fehlt [Bar97].

Ein hoher Grad an Anonymität kann durch digitales Geld im Vergleich zu anderen Zahlungsarten wie z.B. Kreditkartenzahlungen gewährt werden, wobei die einzelnen Systeme dieses Merkmal unterschiedlich stark ausgeprägt realisiert haben. Es folgt die Beschreibung konkreter Beispiele, die diese Unterschiede veranschaulichen.

6.2.1.1 Ecash

Ecash wurde von der Firma DigiCash als anonymes, sicheres, elektronisches, bargeld-ähnliches System zur Anwendung im Internet entwickelt. Es koppelt die Vertraulichkeit von Bargeld mit der Sicherheit, die in offenen Netzwerken wie dem Internet gefordert ist.

Als online Softwarelösung kann es für das Bezahlen von Informationen, physischen Waren und Geschäften mit Rückzahlungsfunktionen eingesetzt werden.

Ecash ist **anonym**, da es keine Möglichkeit gibt, die Herkunft der digitalen Münzen, die über einen speziellen Mechanismus vom Kunden bei seiner Bank abgehoben werden, zu ermitteln. Dieser münzbasierte Ansatz, der Garant für die Anonymität ist, unterscheidet das Ecash-Verfahren grundsätzlich von dem saldenbasierten *CyberCoin*-Verfahren (vgl. Kap. 6.3) [Siet97].

Strenge Sicherheitsvorkehrungen werden im System durch den Einsatz von symmetrischer als auch asymmetrischer Verschlüsselungstechnologie realisiert, und jede Münze wird bei ihrem Transfer bei der ausgebenden Bank auf Echtheit geprüft, was einen zusätzlichen Sicherheitsfaktor darstellt. Es führt jedoch auch dazu, daß die Banken nur ihre eigenen Ecash-Münzen akzeptieren, da sie nur diese prüfen können. Ein **bankenübergreifendes Clearingcenter**, das die im Umlauf befindlichen Ecash-Münzen prüft und verrechnet, ist zur Zeit noch nicht etabliert. Vorstellbar ist, daß die Bundeszentralbank diese Rolle übernimmt.

Das Ecash-Modell geht von einer **Rollenverteilung** der drei Teilnehmergruppen aus [O'Mah97]:

- **Kunde**: kann Münzen von seinem Ecash-Konto abheben und diese in seinem sogenannten *cyberwallet* (lokale Software) speichern. Das *cyberwallet* übernimmt die Verwaltung der Münzen, protokolliert die Transaktionen und wickelt Zahlungen ab.
- **Händler**: prüft erhaltene Münzen bei der ausgebenden Bank auf Echtheit und deponiert diese. Die lokal beim Händler installierte Software wickelt Zahlungen ab.
- **Bank**: gibt eindeutige Münzen aus, validiert diese über eine Datenbank mit dem Bestand der bereits ausgegebenen Münzen, führt Benutzerkonten und löst Münzen ein.

Ecash-Münzen werden vom *cyberwallet* als **Seriennummern** aus sehr großen Zufallszahlen generiert, und dann von der Bank signiert. Die Verwendung von *100-digit-Seriennummern* gewährleistet , daß keine zweite identische Seriennummer generiert wird, bzw. die Wahrscheinlichkeit, daß dieses Ereignis eintritt geht gegen Null. Die Seriennummer wird chiffriert und an die Bank gesendet. Die Bank signiert die Münzen, ohne die Seriennummern zu kennen. Die Software des Kunden dechiffriert die Münzen und prüft, ob die Signatur der Bank erfolgte.

Ein Problem, dieser Methode besteht darin, daß die Bank nicht weiß, über welchen Wert die Münzen ausgestellt sind, da sie die Münzen nur in chiffrierter Form vorliegen hat. Ecash löst dieses Problem, indem die Bank für jeden **Nennwert** der Münzen separate Signaturen verwendet. Der Kunde gibt an, welche Münznennwerte er haben möchte, die Bank unterzeichnet die Seriennummer mit der Signatur, die zum Nennwert paßt und zieht den Betrag vom Kundenkonto ab.

Innerhalb einer Abhebung können Münzen mit verschiedensten Nennwerten angefordert werden. Die Anfrage wird mit dem privaten Schlüssel des Benutzers signiert und dieses

Datenpaket wird nochmals mit dem öffentlichen Schlüssel der Bank verschlüsselt. Der öffentliche Schlüssel der Bank unterscheidet sich von den Schlüsseln, die zur Signatur der Münzen verwendet werden.

Die aktuelle Implementation von Ecash kombiniert symmetrische und asymmetrische Kryptographie-Verfahren zur Steigerung der Effizienz.

Wie andere Formen von elektronischem Geld sind auch Ecash-Münzen nur Datenpakete, die einfach kopiert werden können. Um sicherzustellen, daß eine Seriennummer nicht zweimal ausgegeben wird, bzw. kopiert wurde, wird jede Münze, die bei der Bank wieder eingelöst wurde, in einer Datenbank registriert. Diese zentrale Datenbank, die als Engpaß in Bezug auf die **Skalierbarkeit** des Ecash-System gesehen werden muß, kann sehr groß und damit schwer verwaltbar werden, auch wenn ein Teil der ausgegebenen Münzen, nämlich die deren Gültigkeitsdauer abgelaufen ist, wieder gelöscht werden können. Außerdem ist diese zentrale Datenbank das Hauptkriterium, weshalb jede Bank eigene Münzen ausgibt und nur eigene Münzen einlöst. Dies zieht alle Nachteile der Heterogenität nach sich.

Eine gültige Münze muß also von der ausgebenden Bank signiert sein, ein Gültigkeitsdatum haben, das nach dem aktuellen Datum liegt und darf nicht im Bestand der ausgegebenen Münzen registriert sein.

Sind Münzen auf Grund eines Systemausfalls oder eines Netzwerkfehlers verlorengegangen, können die Münzen, bzw. deren Wert, durch einen Mechanismus wieder hergestellt werden. Teilt der Kunde seiner Bank den **Verlust der Münzen** mit, so schickt diese ihm die exakten Daten der letzten 16 Abhebungen. Der Kunde, der die Verschlüsselungsinformationen der letzten 16 Abhebungen gespeichert hat, entschlüsselt alle Münzen und schickt diese an die Bank zurück, damit sie seinem Konto gutgeschrieben werden. Die Bank vergleicht die Münzen mit dem Bestand der ausgegebenen Münzen und schreibt nur den Betrag der noch nicht ausgegebenen Münzen gut. Der Kunde kann nun wieder neue Münzen anfordern.

Die Einbindung von Ecash ins WWW kann in 9 Schritten beschrieben werden. Abbildung 6-2 veranschaulicht dieses Szenario.

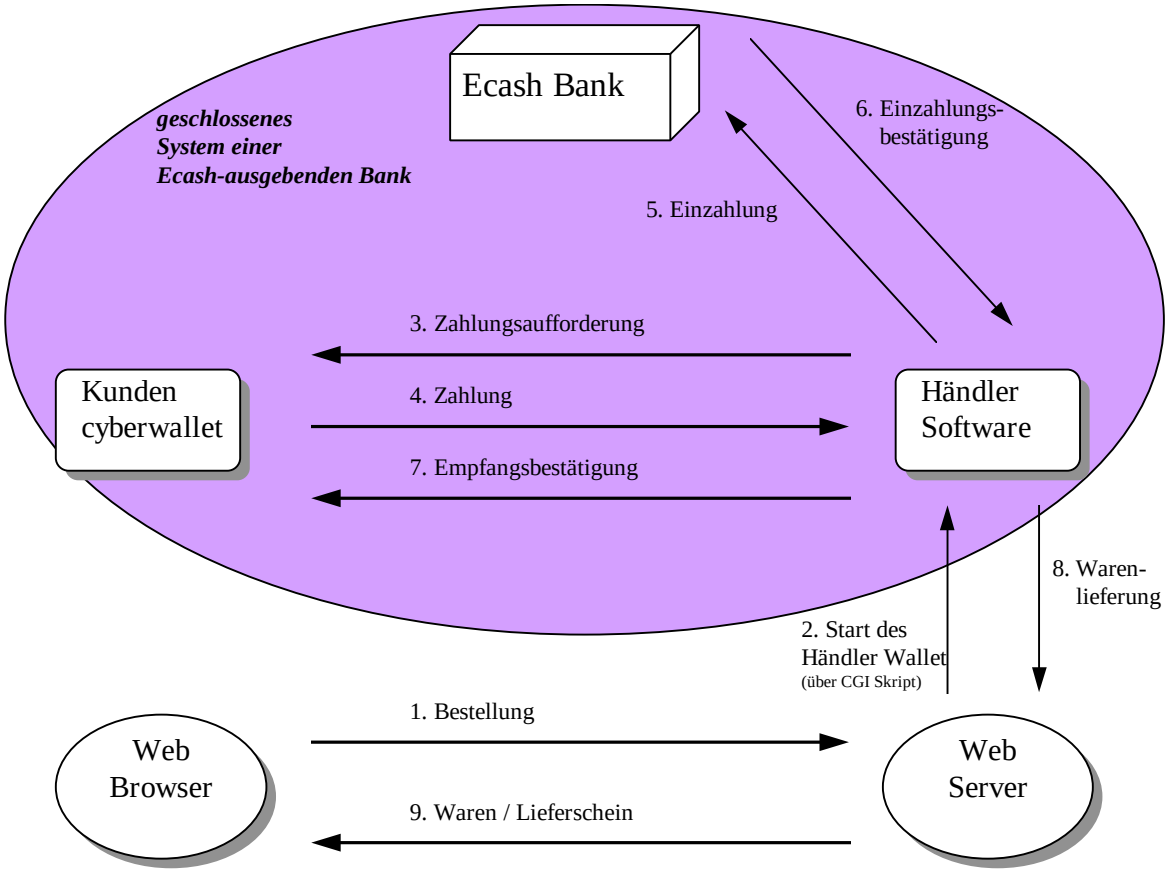


Abbildung 6-2, Einbindung Ecash ins WWW [O'Mah97]

Der Kunde arbeitet parallel mit Web-Browser und cyberwallet. Hat er eine Bestellung auf der Webseite des Händlers selektiert, wird die Ecash Software automatisch über ein *CGI*[15]*-Skript* aktiviert. Das *CGI-Skript* unterstützt den Ablauf eines Programmes auf dem Web-Server und erlaubt die Rückgabe von Ergebnissen über diesen Server. Die Händler Software interagiert mit dem cyberwallet des Kunden. Verlief der Zahlungsvorgang erfolgreich, wird die Vollzugsmeldung an den Web-Browser des Kunden über das WWW gesendet. Diese Methode hat den Vorteil, daß sie mit den meisten Web-Browsern einfach zu integrieren ist.

Ecash Zahlungen können auch über **E-Mail** erfolgen. Der Händler würde in diesem Fall seine Bank evtl. auch über E-Mail kontaktieren und die Münzen auf sein Konto einzahlen. Auch von Nutzer zu Nutzer kann Ecash übertragen werden (*Peer-to-Peer)*,

[15] CGI - **C**ommon **G**ateway **I**nterface

wie reales Bargeld. Um in diesem speziellen Fall die Echtheit der Münzen zu prüfen, tauscht der Zahlungsempfänger diese bei der Bank ein und erhält neu Münzen.

In den USA wird Ecash schon seit 1995 kommerziell eingesetzt und von der Mark Twain Bank angeboten. Weitere kommerzielle Anbieter sind die Merita Bank (Finnland) und die Deutsche Bank AG, die 1997 einen deutschlandweiten Feldversuch gestartet haben [ECIN98].

> Ecash kommt den Anforderungen, die aus der Bargeldähnlichkeit abgeleitet werden, am nächsten. Kein anderes System hat bisher den Anspruch auf **Anonymität** in dem Maße umgesetzt wie Ecash. Da die Firma DigiCash ein Patent auf die beschriebene Methode und das Verfahren von Ecash hält und bisher keine Lizenzen für diese Technologie vergeben hat, kann davon ausgegangen werden, daß in nächster Zeit kein ähnliches System in den Markt drängen wird.

6.2.1.2 NetCash

NetCash wurde vom Information Science Institute (ISI) der University of Southern California als identifizierendes *online electronic cash system* für offene Netzwerke entwickelt. NetCash kommt im elektronischen Zahlungssystem *NetBank*[16] zum Einsatz, deren Philosophie NetCash mit dem Einsatz einer Fremdwährung vergleicht.

Das System besteht aus **verteilten Zahlungsservern**, die elektronische Münzen prägen und diese im Austausch für elektronische Schecks ausgeben. NetCash nutzt die elektronische Scheckinfrastruktur, um monetäre Werte in das System einzubringen und zurück zu transferieren. Der Kunde bezahlt also mit elektronischen Schecks und erhält NetCash Münzen dafür. Die Server untereinander gleichen ihre Konten ebenfalls über elektronische Schecks aus. Das Clearing zwischen den Zahlungsservern läuft über gegenseitig eingerichtete Verrechnungskonten. Alle akzeptierten Schecks werden gesammelt und am Tagesende über die *NetCheque*-Infrastruktur abgerechnet.

Das System ist identifizierend, im Sinne von **nicht anonym**, da jede Münze eine eindeutige Seriennummer hat, die dem Erstbesitzer zugeordnet werden kann. Die Möglichkeit, gültige Münzen bei einem Zahlungsserver gegen neue einzutauschen, erlaubt eine stark eingeschränkte Anonymität.

NetCash setzt keine spezielle Hardware zur Gewährleistung der **Sicherheitsansprüche** ein, sondern löst diese Anforderungen softwareseitig unter Verwendung von symmetrischen als auch asymmetrischen Verschlüsselungsverfahren. Alle Teilnehmer, dies sind der Käufer, der Händler und der Zahlungsserver, müssen ein eigenes, öffentliches-privates Schlüsselpaar besitzen. Die eingesetzten verteilten Zahlungsserver ermöglichen die Skalierung des Systems je nach Benutzeranzahl und Frequentierung. Jede Münze muß während der Zahlungsphase von einem NetCash Zahlungsserver geprüft werden, was bei einer starken Frequentierung zu Engpäßen führen kann.

---

[16] http://www.teleport.com/~netcash

Der Server stellt dem Benutzer die ***vier Dienste*** zur Verfügung:

- **Prüfung** der Münzen, um mehrfach ausgegebene Münzen zu erkennen.
- **Ausgabe** von Münzen, die mit einem elektronischen Scheck bezahlt werden.
- **Rückkauf** der Münzen, deren Wert mit einem elektronischen Scheck erstattet wird.
- **Umtausch** von gültigen Münzen in neue Münzen.

Die Mehrfachverwendung (***double spending***) von Münzen ist auch hier ein großes Sicherheitsrisiko, da eine Münze lediglich durch ein Datenbündel repräsentiert wird und einfach zu kopieren ist. Bei NetCash können nur Münzen, deren Seriennummer in der Datenbank enthalten sind, gültig sein. Wird eine Münze zur Prüfung vorgelegt, wird sie aus dem Datenbestand gelöscht, da sie entweder in einer Zahlungs- oder Umtauschtransaktion verwendet wurde.

Münzen können von einer Person zu anderen übertragen werden (**peer-to-peer**). Vertraut der Empfänger dem Münzbesitzer, so muß der Zahlungsserver nicht zwingend zur Validierung der Münzen hinzugezogen werden. Es müssen jedoch alle Münzen dem Zahlungsserver zum Umtausch vorgelegt werden, bevor das Verfalldatum abläuft. Über das Verfalldatum wird ein Rücklaufmechanismus der elektronischen Münzen in Gang gesetzt, um das Volumen an ausgegebenen Münzen und deren Umlaufgeschwindigkeit innerhalb eines Zeitfensters zu steuern.

Die Umtauschfunktion gewährleistet keine vollständige Anonymität, wie dies z.B. bei Ecash gewährleistet ist, da die Kommunikation über eine Netzwerkadresse läuft, die wiederum Rückschlüsse auf den Münzinhaber zuläßt, es sei denn ein *Proxy Server* wird zwischen geschaltet. Sobald jedoch Münzen gegen einen Scheck eingelöst werden, muß der Benutzer seine Identität preisgeben. Dem Händler gegenüber ist der Käufer nur über seine Netzwerkadresse bekannt.

Das NetCash Protokoll sieht vor, daß Zahlungsserver den Umtausch von Münzen unterbinden können. Dies hätte zur Folge, daß den Kunden des Servers auch keine eingeschränkte Anonymität mehr angeboten werden könnte. Das Käufer-Händler-Verhältnis würde hierdurch jedoch nicht beeinflußt.

Die Problematik der Zertifizierungsinstanzen für die Zertifikate der Zahlungsserver ist zur Zeit noch nicht gelöst, sollte das System in die Pilotphase kommen, müssen hierfür Lösungen gefunden werden.

> Die fehlende Anonymität im NetCash System und die Speicherung privater, sensitiver Informationen auf den zentralen Servern kann zu Datenschutzproblemen führen. Dies ist als größte Hürde für die breite Akzeptanz des Systems einzustufen. Da NetCash zum jetzigen Zeitpunkt nur in Pilotprojekten eingesetzt ist, ist auch für die nahe Zukunft, keine ernsthafte Konkurrenz des Systems zu Ecash zu erwarten.

6.2.2 Kreditkartenbasierte Systeme

Kreditkartensysteme sind seit ca. 1960 als Zahlungssysteme eingeführt und haben eine beachtliche weltweite Verbreitung [O'Mah97]. Die ersten *Online-Zahlungen* wurden über die einfache, unverschlüsselte Weitergabe der Kreditkartendaten übers Netz abgewickelt. Diese Zahlungsabwicklung könnte also als Vorreiter für elektronische Zahlungssysteme im Internet angesehen werden.

6.2.2.1 Mail-Order

Eine unverschlüsselte Übertragung der Kreditkartendaten im Klartext über das Internet stellt den einfachsten Ansatz eines Zahlungsvorgangs dar, birgt verständlicherweise aber auch die größten Risiken für den Kunden und den Händler.

- Der **Händler** trägt das Risiko **gefälschter Kreditkartendaten**. Betrachtet man das Szenario, für das sich ein solcher Mißbrauch eignet, ist der „Einsatzbereich" zwar eingeschränkt, da nur Waren oder Dienstleistungen, deren Distribution über das Internet abgewickelt wird, besonders gut geeignet sind. Bei der Lieferung von materiellen Gütern muß eine real existierende Lieferanschrift mitgeteilt werden. Aufgrund der relativ hohen Transaktionskosten wird die Kreditkartenzahlung von Händlern meist nur für Makropayments[17] angeboten.
- Der **Kunde** nimmt in Kauf, dem Händler gegenüber seine **Zahlungsdaten offenzulegen**. Während bei SET (vgl. Kap 6.1.3) der Händler nur die Bestelldaten einer Transaktion lesen kann, stellt dieses Verfahren für den Kunden keine Möglichkeit zur Verfügung, dem Händler gegenüber anonym zu bleiben [Stol97]. Die Sicherheit des Systems hinsichtlich der Übertragung der Daten wird vom Händler vorgegeben und kann vom Kunden meist nicht überprüft werden.

Kreditkartendaten im Netz **illegal abzuhören** und diese dann für Kauftransaktionen einzusetzen, stellt kaum eine Schwierigkeit dar. Methoden, um an Kreditkartendaten von Internet-Usern zu gelangen (z. B. *Paketsniffer*[18]), sind hinreichend bekannt. Die Gefahr des Sammelns von Kreditkartendaten besteht jedoch seit der Einführung der Kreditkarte, da alle für eine Zahlung relevanten Daten im Klartext auf der Karte vermerkt sind. Erst die Tatsache, daß diese Daten in großem Umfang und mit wenig Aufwand gesammelt werden können, bewegt die Gemüter. Das Ausmaß des Betruges kann also einen ungleich größeren Schaden anrichten, bevor dieser entdeckt und über die gesperrte Kreditkartennummer gestoppt werden kann. Ungeachtet dieser Fakten hat sich diese Art der Zahlung im Internet verbreitet, wohl auch weil sicherere Zahlungssysteme nicht zur Verfügung standen.

---

[17] Makropayments bezeichnen im Gegensatz zu Micropayments Zahlungstransaktionen die in höheren Preissegmenten eingesetzt werden. Die Grenze zwischen Makro- und Micropayments ist in der Literatur nicht einheitlich, wird aber meist bei ca. 15,- DM angegeben.

[18] Methode zur Ausführung eines „..recht primitiven Angriffs auf eine Übertragung, bei der der Hacker einzelne Daten-Pakete während der Übertragung abhören, ausspähen und gegebenenfalls manipulieren kann. Besonders problematisch, wenn die Übertragungsdaten (z.B. Kreditkarteninformationen) im Klartext, also unverschlüsselt, übertragen werden." [Stol97, S.157]

Wird für die Übermittlung dieser sensitiven Daten ein sicherer Kanal verwendet, bzw. ein geeignetes Verschlüsselungsverfahren, so kann das Sicherheitsrisiko des unerlaubten Abhörens enorm verringert werden.

6.2.2.2 First Virtual

First Virtual war eines der ersten kreditkartenbasierten Systeme im Internet, zunächst konzipiert für den Vertrieb von immateriellen Wirtschaftsgütern. Das bestimmende Charakteristika dieses Systems ist die Einbindung eines **vertrauenswürdigen Dritten** (*Trustcenter First Virtual*) und die nur **einmalig erforderliche Übermittlung der Kreditkartendaten** über einen sicheren Kanal außerhalb des Internets.

Der Käufer übermittelt seine E-Mail Adresse, Name des Kreditkarten-/Kontoinhabers etc. an First Virtual und erhält eine sogenannte *VirtualPIN*. Alle diese Informationen können über das Netz ausgetauscht werden. Im nächsten Schritt teilt der Käufer, via Telefon oder Fax etc., First Virtual seine sensitiven Kreditkarteninformationen zusammen mit seiner VirtualPIN mit, so daß First Virtual in der Lage, ist eine Verbindung zwischen der im offenen Netz kommunizierten VirtualPIN und der Kreditkartennummer, die im Internet nicht publik wird, herzustellen.

Der Bezahlvorgang selbst wird vom Käufer initiiert, indem er seine VirtualPIN zusammen mit der Bestellung an den Händlerserver schickt. Der Händler autorisiert den Käufer, indem er die VirtualPIN über den First Virtual-Server prüft. Ist die VirtualPIN gültig, liefert der Händler über E-Mail, WWW oder andere Distributionskanäle an den Käufer aus. Zusätzlich verschickt der Händler die Transaktionsdaten und die VirtualPIN des Käufers an das Trustcenter von First Virtual, das eine E-Mail Anfrage an den Käufer generiert, ob die Waren zur Zufriedenheit geliefert wurden. Streng nach dem Grundsatz „***erst die Ware, dann das Geld***“, wurde bis zum jetztigen Zeitpunkt noch keine Zahlung vorgenommen. Der Käufer hat verschiedene Möglichkeiten, auf die E-Mail-Anfrage zu antworten:

- **accept** - die Zahlung wird ausgeführt
- **reject** - die Waren wurden nicht geliefert oder der Käufer ist nicht bereit zu bezahlen
- **fraud** - es liegt ein Betrug vor, der Käufer hat die Waren nicht bestellt. In diesem Fall wird die VirtualPIN sofort auf eine *schwarze Liste* gesetzt und wird nicht mehr akzeptiert

Auch dieses System hat **Sicherheitslücken**, es besteht die Möglichkeit mit einer gestohlenen Kreditkartennummer eine VirtualPIN anzufordern und über ein kontrolliertes E-Mail-Account die *Bestätigungs-Mail* abzufangen. Außerdem werden, bedingt durch die Kommunikation via E-Mail, für die Kontrolle der Leistungserbringung, betrügerische Handlungen oft erst nach einigen Stunden oder sogar Tagen entdeckt.

Vorteile:
Der größte Vorteil des First Virtual System liegt darin, daß zu keinem Zeitpunkt reale Kreditkartendaten auf dem Rechner gespeichert oder übers Internet übertragen werden.

Ein weiterer Vorteil ist in der Einfachheit des Systems zu sehen. Da keine Verschlüsselungstechnologien eingesetzt werden, bestehen auch keine Exportbeschränkungen und da nur auf E-Mail als Übertragungsprotokoll zurückgegriffen wird, muß weder auf Händler- noch auf Käufer-Seite eine spezielle Software installiert werden.

Nachteile:
Nachteile ergeben sich durch die relativ umständliche Registrierung und den Umstand, daß ein Bank- bzw. Kreditkartenkonto vorhanden sein muß. Zudem entstehen hohe Transaktionskosten, da Händler und Käufer mit einer zusätzlichen Gebühr von First Virtual belastet werden.

> Das System ist bereits seit Ende 1994 in Betrieb [ECIN98], kann aber bisher nur in US-Dollar verwendet werden. Die Besonderheit von First Virtual, daß der Käufer die Ware erhält und erst dann entscheidet, ob er bezahlt, macht das System für Käufer besonders attraktiv, da der Händler das Risiko trägt.

6.2.3 Scheckbasierte Systeme

Scheckzahlung ist in den USA sehr populär, in europäischen Ländern hingegen ist ein eher **rückläufiger Trend** für Scheckzahlung zu erkennen. Dieser rückläufige Trend wird von den Banken noch unterstützt, da die Verarbeitung von beleghaften Schecks (Transport der Belege, Rückweisung geplatzter Schecks, etc.) hohe Kosten verursacht und die Bezahlung mit *Debitkarten* all die Vorteile der Scheckzahlung ermöglicht, jedoch die aufgeführten Nachteile nicht mit sich bringt.

Es gibt verschiedenste Ansätze für die Einführung eines scheckähnlichen, elektronischen Zahlungssystems im global ausgerichteten Internet, bei dem Beträge vom Käuferkonto auf das Verkäuferkonto zum Zeitpunkt des Geschäftsabschlusses transferiert werden. Aus Sicht der Banken wäre die Nutzung der bestehenden Netzwerke für Zahlungssysteme wünschenswert.

6.2.3.1 NetBill

Das Zahlungssystem NetBill wurde von der Carnegie Mellon University und Visa International für Niedrig-Preis-Informations-Güter entwickelt. Das System stellt sicher, daß der Käufer zahlt, wenn er die verschlüsselten Informationen erhalten hat, aber erst nach geprüfter Zahlung den zum entpacken benötigten Schlüssel erhält. Die Mißbrauchsmöglichkeiten sind hierdurch stark eingeschränkt [Stol97].

Der **Ablauf einer Transaktion** kann in acht Schritten beschrieben werden:

1. Hat sich der Käufer für ein Produkt entschieden, fordert er einen Kostenvoranschlag beim Händler an.
2. Der Händler ermittelt den Preis und schickt sein Angebot an den Käufer.
3. Akzeptiert der Käufer das Angebot, beauftragt dieser sein *Checkbook* (Bibliothek für die Interprozess-Kommunikation), eine Kaufakzeptanz an den *Händler Till* (Gegenstück des Checkbook beim Händler) zu senden. Alternativ besteht die

Möglichkeit, das *Checkbook* so zu konfigurieren, daß es automatisch eine Kaufakzeptanz verschickt, wenn der Betrag unter einem festgelegten Limit ist.

4. Der *Till* transferiert die gewünschte Ware an das *Checkbook*, verschlüsselt mit einem Einmalschlüssel und versehen mit einer Prüfsumme.
5. Das *Checkbook* kann anhand der Prüfsumme die Richtigkeit der übermittelten Daten überprüfen, jedoch die Information noch nicht entschlüsseln. Das *Checkbook* sendet eine signierte elektronische Zahlungsanweisung (*EPO* - electronic payment order) an den *Händler Till*, wenn die Daten als korrekt eingestuft wurden. Ab diesem Zeitpunkt kann der Käufer nicht mehr vom Geschäft zurücktreten.
6. Der Händler schickt die entpackte *EPO* an den NetBill Server. Der Server protokolliert die Transaktion, einschließlich einer Kopie des Einmalschlüssels.
7. Der Server verifiziert die *EPO* und meldet die Autorisierung geprüft oder mit Fehler an den Händler zurück.
8. Der Händler schickt den Schlüssel zum Entpacken der Informationen, zusammen mit der Nachricht des NetBill Servers an den Käufer.

Im Idealfall, der oben beschrieben wurde, muß der NetBill Server für eine Transaktion nur einmal angesprochen werden, diese Vorgehensweise stellt ein schnelles **Antwortzeitverhalten** sicher.

Obwohl beim Design des NetBill Protokoll ein besonderer Augenmerk auf das Antwortzeitverhalten des Servers gelegt wurde, ist dieser dennoch der Flaschenhals, da alle Transaktionen mit dem Server kommunizieren müssen, auch wenn die Beträge noch so klein sind. Da es keine einfache Möglichkeit gibt, die Server-Anwendung zu verteilen, wird diese die Obergrenze der am System teilnehmenden bestimmen.

Das Ziel von NetBill ist die **umfassende Unterstützung** von der Preisverhandlung bis zur Warenlieferung und das Risiko der Geschäftstransaktion auf Händler und Kunde zu verteilen. Für diese Funktionalitäten müssen acht Nachrichten ausgetauscht werden. Der Kommunikationsaufwand ist enorm und schlägt sich auf die **Transaktionskosten** nieder.

6.2.4 Micropayments

Für Micropayments ist das Einsatzgebiet bei der Bezahlung von Kleinstbeträgen zu sehen. Das setzt voraus, daß die Transaktionskosten für die Zahlungsabwicklung sehr gering sind, um ein **adäquates Verhältnis** zwischen Transaktionsvolumen und Transaktionskosten zu gewährleisten.

In dieser Sparte sind besonders Angebote von kostenpflichtigen Informationen über Datenbankabfragen, *pay-per-view*- oder *pay-per-use*-Anwendungen oder auch der Vertrieb von Software anzusiedeln. Micropayments machen manche Geschäftstransaktionen, die bisher nicht angeboten wurden, erst möglich, z.B. den Kauf eines einzelnen Titels einer Musik-CD, den Bezug einzelner Teile, beispielsweise Wirtschaftsteile von Zeitungen, etc.

Die **Sicherheitsanforderungen** an diese Systeme sind, auch aus Performance- und Kostengesichtspunkten, **reduziert** (vgl. Kap. 4.1).

6.2.4.1 Millicent

In den Labors von Digital Equipment Corporation (DEC) wurde das 1995 vorgestellte Micropaymentsystem Millicent entwickelt. Es handelt sich um ein dezentrales, kontobasiertes Verfahren, bei dem Händler oder Broker die Konten der Käufer verwalten. Ein Broker, repräsentiert durch beispielsweise einen Provider, eine Bank oder eine Telefongesellschaft [Lan98], unterhält selbst bei verschiedensten Händlern wiederum Konten. Durch diesen dezentralen Ansatz ist das System gut skalierbar und der Kommunikationsaufwand wird auf ein Minimum reduziert.

Der potentielle **Käufer** deponiert einen Geldbetrag auf seinem Millicent-Konto, das er bei einem Händler oder einem Broker unterhält, und erhält als Gegenleistung verschlüsselte Nachrichten (*Scrips*), die für einen bestimmten Zeitraum gültig sind. Mit diesem *Scrip*, der händlerspezifischen Millicent-Währung, kann er bei dem Händler bezahlen. Der Nennwert eines *Scrips* ist frei wählbar und kann beliebig klein gewählt werden, z. B. ein Zehntel eines Pfennigs [mill.com].

Wird über einen **Broker** vermittelt, obliegt es dem Broker, welche Informationen über den Kunden er an den Händler weiterleitet. Da Millicent grundsätzlich die Möglichkeit vorsieht, Boni zu vergeben und Rabattsysteme bzw. Rabattkategorien einzubinden, ist die Übermittlung von personenbezogenen Daten für den Käufer oft von Vorteil. Dem Broker, als *Accounting-Intermediär* zwischen Kunde und Anbieter, fällt eine wichtige vertrauensbildende und Sicherheit gewährende Rolle im System zu [Him96].

Generell läßt sich Millicent mit anderen Zahlungssystemen kombinieren. In der Spezifikation werden keine Vorgaben gemacht, wie ein Betrag auf das Millicent-Konto deponiert wird, hier können die in den vorangestellten Kapiteln beschriebenen Makropayments eingesetzt werden.

> Millicent besticht durch seine Einfachheit und wird als eines der effizientesten elektronischen Zahlungssysteme hinsichtlich der Transaktionskosten gesehen [Stol97]. Außerdem ist es relativ schnell, da ein zentraler Validierungsprozess fehlt.
>
> Der **Schwachpunkt** des Systems liegt jedoch genau in dieser Dezentralisierung, da das Problem der Validierung auf den Käufer abgewälzt wird und er zudem die unterschiedlichsten Scrips für unterschiedliche Händler oder Broker vorhalten muß [Herz98]. Für die Abrechnung von vielen Kleinstbeträgen mit einem Händler ist das Abrechnungssystem bestens geeignet, nicht jedoch für sporadische Käufe bei verschiedensten Händlern.

6.2.4.2 T-Online Billing System

T-Online, germany.net und auch CompuServe oder AOL Bertelsmann Online haben die Möglichkeit, in ihrem geschlossenen Netz diverse Zusatzleistungen direkt mit ihren Kunden, über deren monatliche Gebührenrechnung, abzurechnen.

T-Online, die seit 1. Januar 1998 unter dem Namen Deutsche Telekom Online Service GmbH firmiert, ist mit 1,9 Millionen Kunden der mitgliederstärkste Online-Service in Deutschland, gefolgt von AOL mit 500 000 und CompuServe mit 300 000 Teilnehmern [spie30/3/98]. Für den durchschlagenden Erfolg von T-Online ist nicht zuletzt der Umstand verantwortlich, daß in der Vergangenheit der geschlossene T-Online-Dienst als exklusive Service-Infrastruktur für Homebanking-Anwendungen gewählt wurde. Mit der Öffnung des HBCI Standards für das Internet wird sich diese Situation ändern.

Die Zahl der Bankkonten mit *Online-Zugriff*, die über den T-Online-Dienst geführt werden, hat sich von 1,8 Millionen 1996 auf 3,5 Millionen elektronisch geführter Bankkonten fast verdoppelt [spie19/1/98]. Die Bestrebung, den T-Online Kunden einen komfortablen Zugang zum Internet zu ermöglichen, was auch die Abrechnung von kostenpflichtigen Online-Angeboten mit einschließt, wird den bestehenden Wachstumstrend noch verstärken.

Für die Kunden der Online-Dienste werden bei der Anmeldung **Gebührenkonten** eingerichtet und die Modalitäten der Zahlungsabwicklung ausgehandelt. Zwischen Kunde und Online-Dienste-Anbieter besteht bereits ein Vertragsverhältnis, das als Basis für die Abwicklung von Zahlungen herangezogen wird. Der Abrechnungsdienst der T-Online, auch *TOB (T-Online Billing*) genannt, beschränkt sich auf **Micropayments**. T-Online hat eine Spanne von 1 Pfennig bis 9,99 DM für die Abrechnung von zusätzlichen Leistungen festgelegt [c't 16/97]. TOB wird überall dort wirtschaftlich eingesetzt, wo Klein- bzw. Kleinstbeträge verrechnet werden, wie z.B. beim Abruf von Informationen, dem Download von Dokumenten oder Dateien etc.

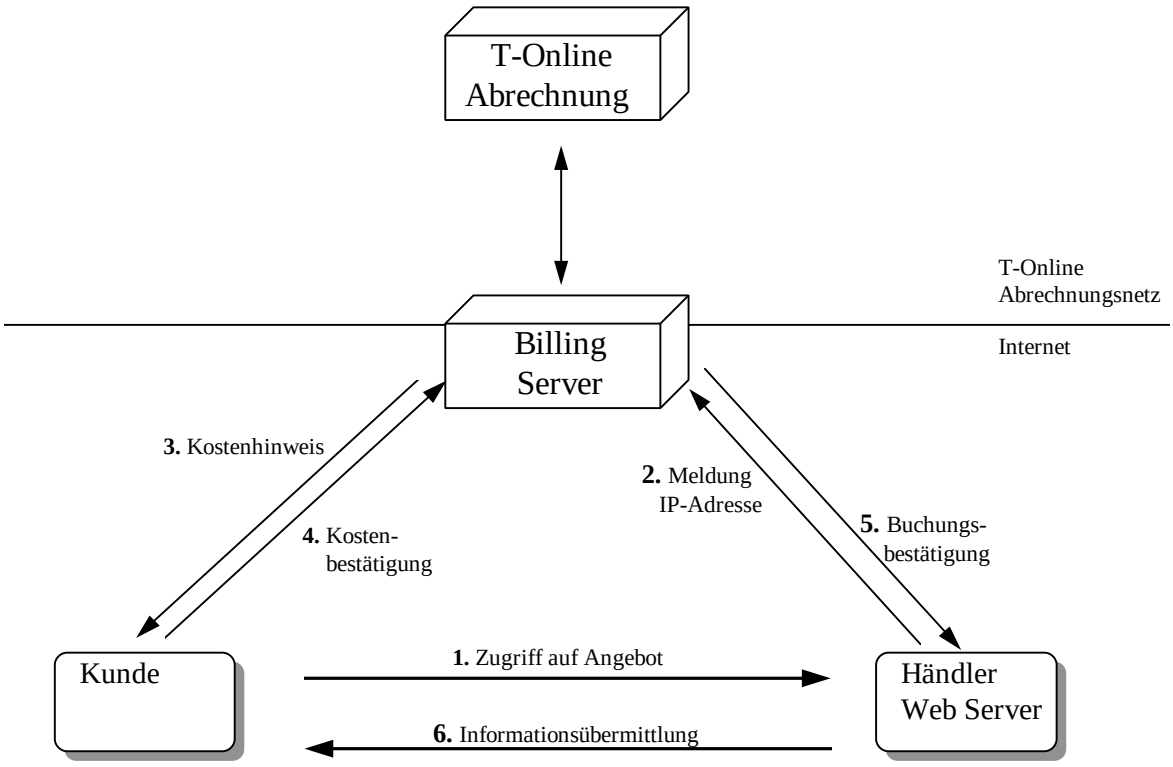


Abbildung 6-3; Abrechnung von Internetangeboten über den Billing Server

Nicht der Ablauf innerhalb des T-Online-Dienstes soll hier betrachtet werden, sondern vielmehr das Verfahren, das angewendet wird, um Internet-Käufe abzuwickeln.

Wir betrachten also das Szenario, daß ein Händler sein Angebot auf einem **Webserver** plaziert hat und der Käufer ein T-Online Kunde ist, der über den **Billing Server** abrechnen will. Es entsteht ein Dreiecksverhältnis zwischen Händler, Kunde und Billing Server. Dieses Dreiecksverhältnis wird in Abbildung 6-3 graphisch dargestellt.

Nachdem der Käufer auf den Webseiten des Händlers seine Bestellselektion abgeschlossen hat, werden die IP-Adresse des Käufers und zahlungsrelevante Transaktionsdaten an den Billingserver weitergeleitet. Diese IP-Adressen werden innerhalb der T-Online-Infrastruktur bei der Einwahl des Online-Kunden dynamisch vergeben. Der Billingserver kann die Verknüpfung zwischen temporärer IP-Adresse und identifiziertem Teilnehmer herstellen und sendet eine Kostenbenachrichtigung zur Bestätigung an den Käufer. Hat der Käufer die Kosten bestätigt und somit eine Willenserklärung im juristischen Sinne abgegeben, belastet der Billingserver das Käuferkonto und schreibt den Betrag dem Händlerkonto gut. Der Händler erhält eine Buchungsbetätigung und kann die bestellten Waren übers Netz versenden, bzw. die Auslieferung veranlassen.

Der Nachrichtenversand im Internet wird über das SSL-Protokoll (mit 128-Bit-Schlüssel) gesichert. Als Softwarevoraussetzung ist beim Kunden ein webfähiger Browser und ein spezielles *Plug-In*, das von T-Online geliefert wird, erforderlich. Der Händler Server muß

die IP-Adresse des Kunden lesen können und diese Information zusammen mit seiner Kennung SSL-verschlüsselt an den Billing-Server weiterleiten.

> Nach Aussage von T-Online ist die Veröffentlichung der Schnittstellenformate zum Billing-Server zur Zeit nicht vorgesehen[19] und der praktische Einsatz der Abrechnungsmethode läßt, trotz vieler Pressemeldungen über die, mehrmals verschobenen, geplanten Starttermine, noch auf sich warten.

6.3 CyberCash

CyberCash nimmt eine Sonderstellung unter den Zahlungssystemen ein, da es sich hierbei um ein Verfahren handelt, das unter gleicher Benutzeroberfläche sowohl ein **kreditkartenbasiertes** System als auch ein **münzbasiertes** System (*Cybercoin)* und ein **lastschriftbasiertes** Verfahren (edd)[20] anbietet. Das kreditkartenbasierte Zahlungssystem wurde an SET adaptiert.

CyberCash stellt ein Gateway vom Internet zum etablierten Bankennetz zur Verfügung, den *CyberCash-Server*. Das CyberCash-Modell besteht aus dem *CyberCash-Wallet* (Käufer-Applikation), *Merchant-Software* (Händler-Applikation) und dem bereits erwähnten *CyberCash-Server* der die Prüfung der Kreditkartendaten vornimmt und eine Rückmeldung an die Merchant-Software veranlaßt. Die Anwendungssoftware für den Kunden, das *CyberCash-Wallet*, stellt unter anderem die Funktionalität zur Initiierung eines Kaufs mit der Kreditkarte und verschiedenste Verwaltungsfunktionen zur Verfügung. Die *Merchant-Software* verarbeitet erhaltene Zahlungsdaten und leitet Kreditkartendaten an den CyberCash-Server zur Prüfung weiter.

Um den ***CyberCash-Service*** für **Kreditkartenzahlungen** in Anspruch nehmen zu können müssen sich die Teilnehmer zunächst registrieren lassen mit einer eindeutigen *CyberCash-ID*, welche die Verbindung zu den *public-/private-key-Paar* des Teilnehmers gewährleistet, und einem Paßwort. Zusätzlich zu diesen Sicherheitsvorkehrungen wird beim Kreditkartenaussteller die Freigabe der Karte für Internet-Zahlungen abgefragt. ID und Paßwort werden eingesetzt, um die Wallet-Software zu entriegeln, in der die Kartendaten und geheimen Schlüssel in verschlüsselter Form gespeichert sind. Im Falle eines Mißbrauchs kann über ID und Paßwort ein '*emergency close-out'* vorgenommen werden, um alle weiteren Transaktionen mit dieser Kartennummer zu blockieren.

Der **Bezahlvorgang** als solcher wird vom Käufer angestoßen, indem dieser den 'Bezahl-Knopf' drückt und daraufhin vom Händler die *Payment-Req*, mit den vom Händler unterzeichneten Bestelldaten, erhält. Der Käufer wählt nun Kreditkarte Lieferadresse, etc., die seine Wallet-Software zur Auswahl stellt und verschickt die *credit card payment message* an den Händler. Diese *message* enthält die mit dem öffentlichen Schlüssel des CyberCash-Servers verschlüsselten Kreditkartendaten, die vom Käufer signiert sind,

---

[19] Telefonat am 5.3.1998, T-Online Service Frau Fianden

[20] edd - (**e**lectronic **d**irect **d**ebitting) ist dem POS-Zahlungssystem nachempfunden, bei dem der Kunde mittels einer maschinenlesbaren Karte (meist ec-Karte) Bezahlvorgänge tätigen kann und der Rechnungsbetrag automatisch von seinem Bank-Konto abgebucht wird. Für edd wird eine virtuelle Karte eingesetzt [SaLB.de].

einen über die Bestellinformationen errechneten Hashwert, zur Integritätssicherung, und die weitergeleitete digitale Unterschrift des Händlers.

Im nächsten Schritt erfolgt die sogenannte *Auth-Capture*, in der anhand der Signatur des Karteninhabers die Kartendaten und anhand der Signatur des Händlers die Bestelldaten verifiziert werden. Durch diese Verifikation stellt der Server sicher, daß beide Parteien mit dem Geschäft einverstanden sind. Sind diese Voraussetzung gegeben, werden die Daten im Bankennetzwerk autorisiert und gecleart. Das Gateway sendet die nicht signierten Nachrichten für Händler und Käufer an den Händler, der wiederum die für den Käufer bestimmte Nachricht, die *Charge-Card-Response*, an diesen weiterleitet.

Die *CyberCash-Message* ist protokollunabhängig und kann über *HTTP, SMTP* oder andere Protokolle transportiert werden.

Der Einsatzschwerpunkt für das **CyberCoin-Modell**, dem münzbasierten System innerhalb der CyberCash-Lösung, ist der Bereich von geringwertigen Gütern und Dienstleistungen, bei denen das Bezahlen mit Kreditkarte wirtschaftlich nicht sinnvoll wäre.

In Abbildung 6-4 wird dieses Modell graphisch dargestellt.

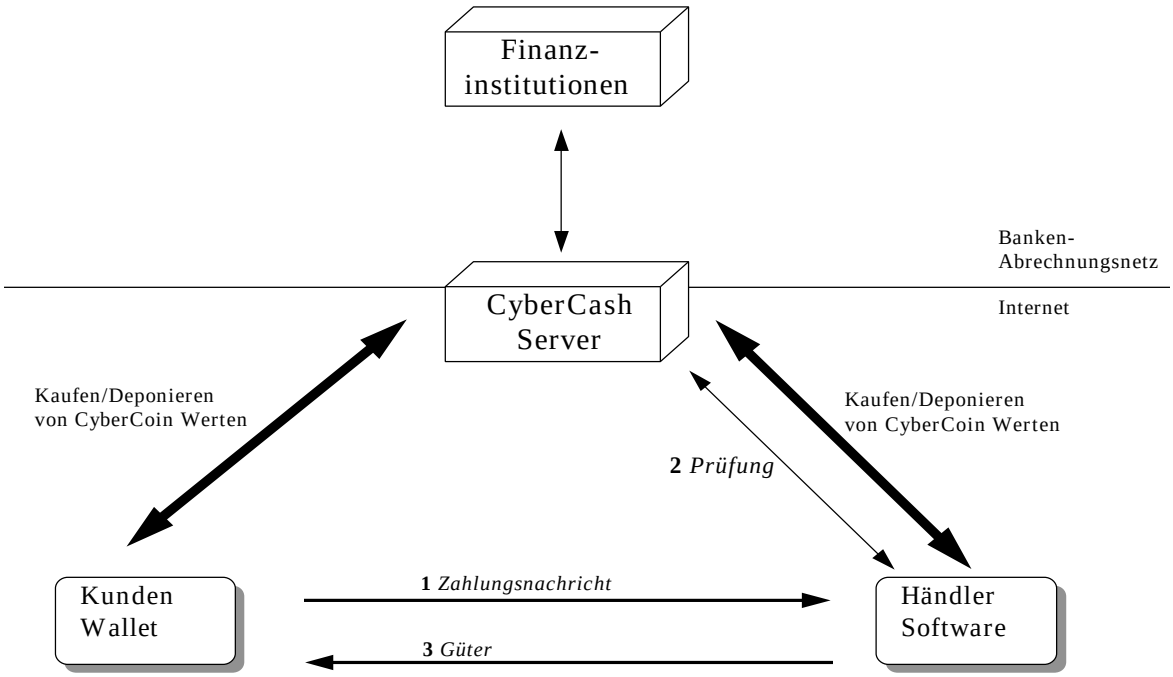


Abbildung 6-4; CyberCoin Modell

Kunden kaufen *CyberCoin Münzen* beim *CyberCash-Server*, der auch deren kreditkartenbasierte *CyberCash-Transaktionen* abwickelt, dem sie also hinlänglich bekannt sind. Die *CyberCoins* werden in einem speziellen Bereich des *CyberCash-Wallet* gespeichert. Der Käufer schickt eine Zahlungsnachricht an den Händler, bleibt dabei jedoch anonym. Das *CyberCash-Wallet* protokolliert alle Transaktionen. Der *CyberCash-Server* kann alle Transaktionen des Käufers nachvollziehen, hier besteht **keine**

Anonymität. In den Protokolldateien des CyberCash-Servers sind sämtliche Daten gespeichert [DrDu98].

Der Händler läßt die Zahlungsnachricht vom *CyberCash-Server* prüfen und verschickt, nachdem er eine positive Rückmeldung erhalten hat, die Güter. Die Verrechnung der Beträge wird vom *CyberCash-Server* übernommen, wobei dieser Kleinstbeträge über einen bestimmten Zeitraum hinweg sammelt und später über das Bankennetz verrechnet.

Das *CyberCoin-System*, bildet die Metapher der elektronischen Münze nur sehr schwach ab. Es ist kein tokenorientiertes System, wie z.B. Ecash, das mit Einheiten von Daten, die einen aktuellen Wert repräsentieren, arbeitet.

CyberCash ist ein proprietäres System, dessen detailliertes Protokoll noch nicht offengelegt wurde. Es nehmen immer drei Parteien an einer Transaktion teil, wobei die CyberCash GmbH immer beteiligt ist. Auch im Pilotprojekt, das dem System für den deutschen Markt einen Imagevorteil bringt, wird das zentrale Zahlungsgateway von einer Gesellschaft betrieben, an der die beiden initiierenden Banken und die CyberCash GmbH beteiligt sind.

Um CyberCoins und die benötigten Schlüssel ins Wallet zu laden, wird public-key-Kryptographie eingesetzt, wie auch bei der Kommunikation zwischen *CyberCash-Server* und der Händler-Software. Im deutschen Pilotprojekt, das die CyberCash GmbH in Zusammenarbeit mit der Dresdner Bank, Sachsen LB, West LB, Hypo- und Vereinsbank, etc. betreibt, wird zusätzlich zur Firewall-Technologie ein Sicherheitssystem mit dem Namen „Advanced Routers“ zur Beobachtung von Unregelmäßigkeiten und Daten zweifelhafter Herkunft eingesetzt [Weis98].

Eine globale Marktplazierung wird mit dem Projekt *„GlobalCoins*“, einer virtuellen Währung, die in USA, in Japan und in Großbritannien eingesetzt werden kann, angestrebt [Schu3/98].

> Das CyberCash-System bietet eine Lösung an, die verschiedenste Zahlungsmittel unter einer gemeinsamen Oberfläche anbietet. Dieser erweiterte Service schwächt die Nachteile, die ein proprietäres System wie CyberCash hat, ab.

6.4 Framework

In den nachfolgend dargelegten Abschnitten werden Frameworks beschrieben, die verschiedene Konzepte zur Gestaltung des E-Commerce skizzieren. Diese Konzepte, die auf offenen Architekturen aufbauen, focusieren nicht ausschließlich Zahlungssysteme, sondern decken den weitgreifenderen Bereich des E-Commerce ab.

6.4.1 SEMPER

Secure Electronic Market Place for Europe (SEMPER) ist ein Projekt, das von der EG-Kommission 1995, als Nachfolgeprojekts von *CAFE* (Conditional Access For Europe), ins Leben gerufen wurde. SEMPER beschäftigt sich vorrangig mit dem **globalen**

elektronischen Handel im Internet und forciert die Entwicklung eines **sicheren Marktplatzes** über das klassisch unsichere Internet.

Nachfolgende **Voraussetzungen** sind für einen sicheren Marktplatz zu definieren [Lac97]:

- Alle Handelstransaktionen des E-Commerce sollten im Marktplatz abbildbar sein, um eine geschlossenen Transaktionskette zu erhalten.
- Die Vertrauensbildung zwischen potentiellen Handelspartnern sollte erleichtert werden. Ein Trust-Netzwerk könnte den Eckstein für einen vertrauensvollen Handel bilden.
- Der elektronische Marktplatz sollte offen für alle, benutzerfreundlich, zuverlässig und rechtssicher sein.
- Der Benutzer muß dem System vertrauen können. Das impliziert auch die Aufklärung des Benutzers über die Bedeutung von E-Commerce und dessen Chancen bzw. Risiken.
- Die komplexen Technologien müssen in ein zuverlässiges, einfach zu handhabendes System eingebunden werden, das interoperabel und von heterogenen Systemumgebungen unabhängig ist.
- Die rechtliche Anerkennung der elektronischen Handelstransaktionen muß grenzüberschreitend gewährleistet sein.

SEMPER sammelt rechtliche, wirtschaftliche, soziale und technische Anforderungen, um sie in einen **ganzheitlichen Ansatz** des E-Commerce miteinfließen zu lassen. Im Gegensatz zu vielen anderen Entwicklungen, deren Bestreben sich auf Segmente von E-Commerce beschränkt, ist SEMPER bestrebt, ein Framework für den globalen elektronischen Handel zur Verfügung zu stellen. Der ganzheitliche Ansatz ist durch die, bisher leider wenig beachteten bzw. umgesetzten, Aspekte des Nutzervertrauens in die Schnittstelle und der Schaffung einer Basis für den fairen Handelsaustausch zwischen den Parteien, z.B. durch das Hinzuziehen eines vertrauenswürdigen Dritten, geprägt. Außerdem müssen Konzepte für die Klärung von Streitfragen und die Gewährleistung einer Mehr-Parteien-Sicherheit entwickelt werden.

SEMPER stellt für diese Aspekte **Services** zur Verfügung, die sich in die Basisdienste, wie z.B. Vertraulichkeit, Authentifizierung, Integrität, Zahlung etc., und die erweiterten Dienste, wie fairer Austausch, Rechtswirksamkeit und sichere Dokumentenverarbeitung, untergliedern.

Dieser Einteilung der Dienste trägt auch die **SEMPER Architektur** Rechnung, die vier funktionale Schichten umfaßt.

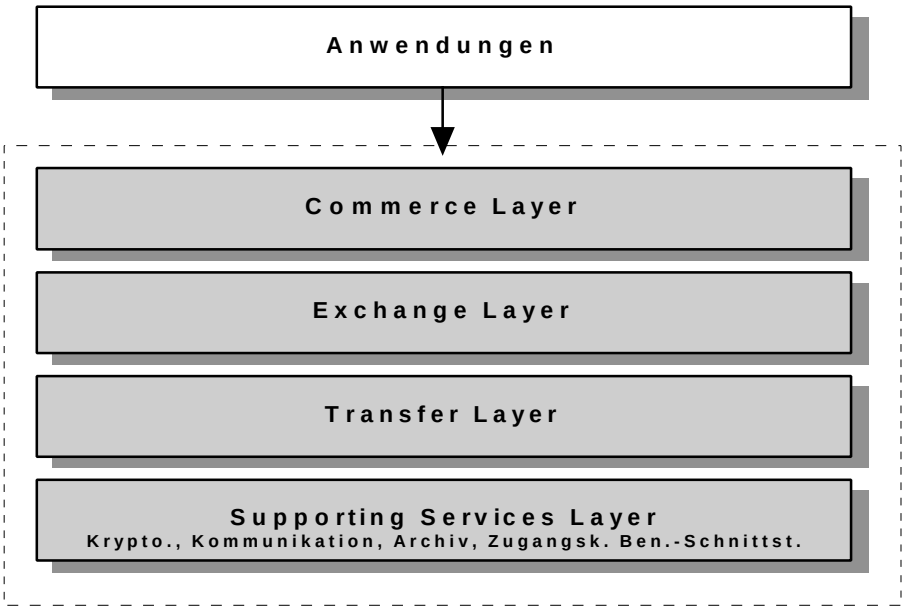


Abbildung 6-5; SEMPER Architektur [Lac97 S.6]

Der ***Commerce Layer*** bietet Dienste an, die direkt die Protokolle der *Geschäftsprozesse*, wie z.B. Angebot, Bestellung, Zahlung, etc., verschiedener Service-Provider implementieren. Außerdem ist ein *Business Application Framework* für Anwendungsentwickler und Designer vorhanden, um den Entwicklungsaufwand zu reduzieren.

Der ***Exchange Layer*** ist für den fairen Austausch zwischen den Handelsparteien verantwortlich. Ein fairer Austausch ist durch das Einverständnis der Parteien über die Geschäftsbedingungen und die vertraglichen Regelungen gekennzeichnet.

Der ***Transfer Layer*** unterstützt das Senden und Empfangen von Informationen, die in Kontainern zusammengefaßt sind. Den Kontainern werden Attribute zugeordnet, die den Übermittlungsweg bzw. die Übertragungsart des Kontainers festlegen.

Der unterste Layer, der ***Support Service Layer*** unterstützt alle anderen Schichten mit grundsätzlichen Diensten, wie z.B. kryptologische Verfahren, Kommunikationsdienste, Protokollierung und Archivierung, Zugangsverwaltung, Benutzerschnittstelle etc.

Die beschriebene Architektur ist im SEMPER-Prototyp implementiert, der vorrangig nachfolgend aufgeführte **Ziele für eine Plattform** verfolgt:

- interoperabel und systemunabhängig
- rechtliche Anerkennung, cross boarder (auch grenzüberschreitend)
- Trust Netzwerke
- Vertrauen des Benutzers
- Einsatz kryptographischer Verfahren

- geschlossene Transaktionskette

SEMPER hat die Freiheit, auf Grund seiner weitgehenden Unabhängigkeit von wirtschaftlichen Interessengruppen, auch Funktionalitäten in ihre Konzepte zu integrieren, die nicht primär kommerziell nutzbar sind. Trotzdem besteht eine enge Zusammenarbeit zwischen SEMPER und Wirtschaftsunternehmen in der Forschung. Es muß also nicht befürchtet werden, daß die Forschungen am tatsächlichen Bedarf vorbeigehen. Vielmehr wird über diese Konstellation sichergestellt, daß auch weniger beliebte oder populäre Themen aufgegriffen werden, Themen, die keinen direkten Nutzen oder Imagegewinn versprechen.

SEMPER hat die Möglichkeit einen ganzheitlichen Ansatz verfolgen zu können, der sozial, wirtschaftlich, rechtlich und technisch anforderungsgerecht gestaltet ist und sich über alle Phasen des elektronischen Handels erstreckt. Die Gestaltung eines sicheren elektronischen Marktplatzes ist mehr als nur die Implementation eines Zahlungssystems. Das Projekt beschäftigt sich auch mit Fragestellungen zu den gesellschaftlichen und politischen Implikationen.

6.4.2 Open Trading Protocol

Das Open Trading Protocol (OTP) ist ein interoperables *Message-Protokoll*, das als offener, flexibler, erweiterbarer und herstellerunabhängiger Standard für die Entwicklung von Software-Applikationen im E-Commerce Bereich konzipiert wird.

Das Open Trading Protocol (OTP) Konsortium bestand im Januar 1998 aus circa 30 namhaften Unternehmen, die diese unabhängige Organisation unterstützen. Ähnlich wie bei der Etablierung von *SET*, *JEPI*[21] oder *EMV*[22], um nur einige zu nennen, wird auch hier ein Business-Modell herangezogen, das auf der **gemeinsamen Spezifikation** eines Standards aufsetzt. Die Teilnehmer profitieren in mehrerer Hinsicht von dieser Zusammenarbeit; zum einen werden vorhandene Entwicklungen bei der Spezifikation mitberücksichtigt und eingebunden, bzw. Schnittstellen definiert, so daß die Investitionen abgesichert werden und zum anderen ist durch die Kooperation der „Marktgrößen“ die Einflußnahme konzentriert und der Standard hat sehr gute Chancen, sich zu etablieren.

Die unterstützten Handelstransaktionen Angebot, Faktura, Zahlungsbeleg-Erstellung und Lieferung sind unabhängig von der Zahlungsmethode [OTP98].

Die zu identifizierenden **Vorteile von OTP** sind [OTP98]:

- **E-Commerce Software-Anbieter** können Produkte entwickeln, die auf Grund ihrer Interoperabilität für den Anwender höchst attraktiv sind. Trotz oder gerade wegen der einheitlichen Plattform hat der Software-Anbieter eine Fülle von Möglichkeiten zur Produktdifferenzierung.

---

[21] **J**oint **E**lectronic **P**ayment **I**nitiative (JEPI) von CommerceNet und W3C (World Wide Web Consortium)

[22] EMV - Standard für den Einsatz von Chipkarten-Technologie, von **E**uropay, **M**asterCard und **V**isa

- **Zahlungssysteme** werden im OTP gekapselt und stehen für die OTP-Anwendungen zur Verfügung, so daß eine Vielzahl von Zahlungssystemen in verschiedensten Anwendungen verfügbar sein werden.
- Der **Händler** kann davon ausgehen, daß auf Grund von inkompatiblen Software-Anwendungen oder Zahlungsmethoden, nicht weniger Aufträge zustande kommen.
- **Banken und Finanzdienstleister** können neue Services für den Händler und Kunden auf der Basis des OTP-Standards anbieten.
- Dem **Käufer** steht eine konsistentere Benutzerschnittstelle zur Verfügung, und es ist eine größere Auswahl an Händlern zu erwarten, mit denen Geschäfte abgewickelt werden können. Durch die Protokollierung der Transaktionen sind Daten verfügbar für die Übernahme in Finanzanwendungen oder evtl. zur Vorlage in Steuerangelegenheiten, wenn das Finanzamt diese, mit digitaler Signatur versehenen Transaktionsbelege, akzeptiert.

Die genannten Vorteile ergeben sich aus dem **Zusammenspiel der Teilnehmer** innerhalb der Handelsarchitektur von OTP, wobei die Verteilung der fünf unterschiedlichen Rollen nicht zwingend auf unterschiedliche Teilnehmer erfolgt. Der Händler kann zum Beispiel die Lieferung selbst abwickeln oder einen Dritten als Lieferanten einsetzen usw. Abbildung 6-6 verdeutlicht das Zusammenspiel der Handelsarchitektur-Teilnehmer .

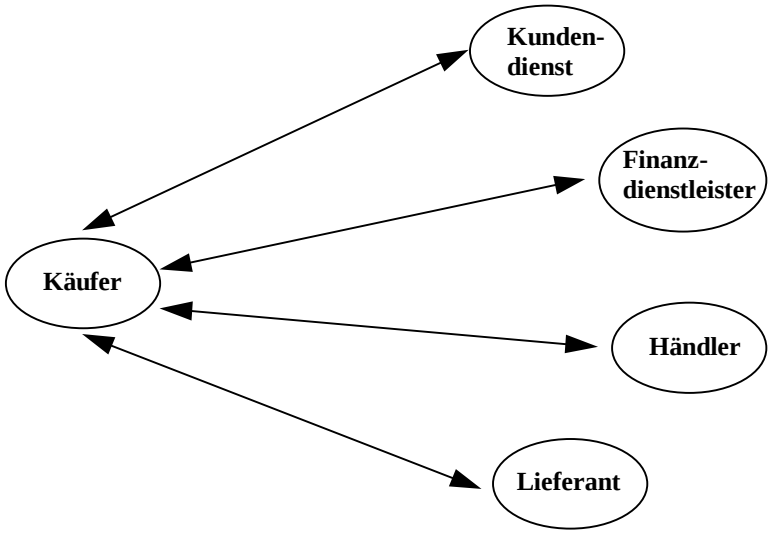


Abbildung 6-6; OTP Architektur [OTP98]

Ein vorrangiges Ziel von OTP ist die **Komplementierung** - nicht der Austausch - bestehender Protokolle oder Zahlungsmechanismen in der IT unterstützten Handelstransaktionskette. Das Protokoll baut auf *XML*[23] auf, einem sich herausbildenden

[23] E**x**tensible **M**ark Up **L**anguage (XML); http://www.w3.org/TR/PR-xml-971208

Standard für den Informationsaustausch im Internet. Die Kapselung der bestehenden Zahlungsmethoden stellt die Unabhängigkeit des elektronischen Handels vom gewählten Zahlungsmechanismus sicher.

Werden Dritte in die Abwicklung des Handels einbezogen, muß die Informationsversorgung über den Status der verschiedenen Transaktionen gesichert sein. OTP hat für das Überwachen der Statusinformationen zusätzliche Abfragetransaktionen eingeführt, die über den Fortschritt der Transaktionsabwicklung jederzeit Auskunft geben.

Der OTP-Standard ermöglicht die Entwicklung eines konsistenten Frameworks von vielfältigen Formen des E-Commerce. Sowohl Analogien zu den Handelsmodellen in der realen Welt als auch neue, aus der Ubiquität des Mediums resultierende Modelle von globaler Interoperabilität werden von OTP unterstützt. OTP unterscheidet mehrere **Handelsmodelle** hinsichtlich des Zahlungszeitpunkts:

Handelsform	Ausprägung und Zahlungszeitpunkt
Nachnahme	Dies ist eine der weitverbreitetsten Handelsformen in der realen Welt, bei der die Zahlung erst eingeleitet wird, wenn die Ware geliefert wurde. Der Händler trägt hierbei das Risiko, die gelieferte Ware vom Kunden nicht bezahlt zu bekommen.
Vorauszahlung	Bei der Vorauszahlung oder Vorauskasse erfolgt die Lieferung der bestellten Waren erst nach dem Eingang der Zahlung bzw. der Zahlungsbestätigung. Der Käufer trägt hierbei das Risiko, die bezahlte Ware nicht geliefert zu bekommen.
parallele Zahlung und Lieferung	Bei diesem Handelsmodell erfolgt die Zahlung und Lieferung zeitgleich. Für Verkäufer und Käufer verkürzt sich die Durchlaufzeit, da nicht auf die Vollzugsmeldung von Zahlung bzw. Lieferung gewartet werden muß. Der Käufer trägt hierbei das Risiko für ein nicht lieferbares Produkt bezahlt zu haben.
Abschlags-zahlungen	Das Handelsmodell mit Abschlagszahlungen hat die Charakteristika eines Zug-um-Zug-Geschäfts. Zunächst leistet der Käufer eine Anzahlung und erhält die Lieferung oder eine Teillieferung mit der Forderung nach einer Abschlagszahlung für die nächste Teillieferung. Dieser Ablauf wiederholt sich bis der Handel abgeschlossen und die Forderungen ausgeglichen sind.
Zahlung je Zeiteinheit	Bei diesem Modell erfolgt die Zahlung je Zeittakt über die gesamte Nutzungsdauer.

Die oben aufgeführten Handelsmodelle sind nicht alle im OTP-Standard definiert, obwohl dies wünschenswert wäre. Es besteht jedoch die Möglichkeit, über Parameter Handels-

Protokoll-Optionen zu setzen, die auf Grund unterschiedlicher Sequenzen von Ereignissen optionale Verarbeitungsschritte einleiten.

Um die **Integrität** der übermittelten Informationen sicherzustellen, setzt OTP Signaturen und Hash-Algorithmen ein. Für den Käufer ist keine public-key-Infrastruktur notwendig, da es in der Grundausbaustufe von OTP keine obligatorische Prüfung der Käufersignatur gibt, wohl aber zwischen Teilnehmern, Händlern, Finanzdienstleistern und Lieferanten. Die verwendeten Signaturen innerhalb der Zahlungssysteme bleiben hiervon unberührt, da diese Daten, bis auf die generischen Zahlungsdaten, gekapselt sind.

Die **generischen Daten** in einem Zahlungsdatenschema sind dadurch gekennzeichnet, daß sie in allen Zahlungssystemen vorkommen, wie z.B. der Händlername oder Zahlungsbetrag etc. Im Gegensatz dazu sind Daten zu identifizieren, die spezifisch für ein Zahlungssystem sind, und nur dort vorkommen.

> Wie auch SEMPER ist OTP nicht auf ein Zahlungsschemata beschränkt, sondern deckt den gesamten Bereich des E-Commerce durch eine offenen Architektur ab. Dies ist der zentrale Punkt für die Integrationsfähigkeit zu bestehenden Anwendungen und zukünftig realisierbarer Geschäftskonzepte, deren Anforderungen zum jetzigen Zeitpunkt noch nicht bekannt sind.

6.5 Zusammenfassung

Im folgenden werden die beschriebenen Systeme zusammengefaßt und miteinander verglichen.

Primär handelt es sich bei **HBCI** nicht um ein Protokoll für Internet-Zahlungsmittel, sondern für Homebanking-Anwendungen. Die Bestrebungen der deutschen Bankverbände gehen jedoch dahin, das Protokoll auch für Zahlungssysteme einzusetzen und so ein Verschmelzen der beiden Anwendungsschwerpunkte *Homebanking* und *Online-Bezahlen* zu ermöglichen. Der Ansatz hierfür einen einheitlichen Standard zu etablieren, ist zu begrüßen, wobei es fraglich ist in welchem Umfang dieser, zunächst auf Deutschland - also national - beschränkte Standard akzeptiert wird. Zumal SET als Standard schon fest am Markt etabliert ist.

Die Teilnahme des SIZ an den Standardisierungsbestrebungen von **OTP**, im Bereich der Chipkarten-Abwicklung nach HBCI-Standard, bereiten eventuell einen Weg für die internationale Ausrichtung. Man kann zu dem Schluß kommen, daß OTP durch seinen globalen, von namhaften Unternehmen getragenen, offenen Ansatz, gute Erfolgsaussichten hat, sich als Standard zu etablieren. Ob sich diese Einschätzung bewahrheitet, hängt besonders von den Ergebnissen der ersten Pilotinstalationen ab, die noch aussteht.

SET hat sich als Standard im Bereich Kreditkartentransaktionen durchgesetzt und damit wird **iKP** als Zahlungsprotokoll kein großes Marktpotential mehr erlangen. Für den Erfolg von SET ist einerseits der umfangreiche Sicherheitsmechanismus und andererseits die

Vertrauensbasis, in der Abwicklung von Kreditkartentransaktionen, und die finanzielle Kraft der Initiatoren VISA und Mastercard verantwortlich zu machen.

Eine weiteres mögliches Szenario wäre die **Integration von HBCI in den SET-Standard**, wie dies in der Entstehungsgeschichte von SET mit anderen Konzepten schon zu beobachten war. HBCI könnte den Bereich der Überweisungen und kontobezogenen Geschäftsvorfälle innerhalb von SET abdecken, respektive SET um Homebanking-Funktionalitäten erweitern.

CyberCash ist eine sehr interessante, obwohl proprietäre, Lösung mit eigener Mehrwert-Dienste-Philosophie. Durch das Zusatzangebot von Makro- und Micropayments erreicht CyberCash eine höhere Flexibilität, sowie eine breitere Segmentabdeckung. Durch die Implementation von SET wird zudem, das SET entgegengebrachte Vertrauen auch auf CyberCash projiziert, was eine Erhöhung des Marktanteils mit sich bringen könnte. Das System unterscheidet sich von anderen abgegrenzten Zahlungssystemen, so daß CyberCash eher als Lösungsanbieter für Zahlungssysteme, denn als univalentes Zahlungsmittel eingestuft werden muß. Nach der anfänglichen Euphorie wurde der Zeitplan korrigiert und die kommerzielle Phase wird noch in diesem Jahr eingeleitet [Schu5/98].

Im Bereich **Micropayments** ist noch nicht abzusehen, welche Systeme sich durchsetzen, und ob die vielversprechenden Prognosen für diese Systeme eintreten werden. Bei der Unternehmensbefragung im Rahmen der „Electronic Commerce Enquete“ gaben 55 % der Befragten an, die Abwicklung von Kleinstbeträgen sei organisatorisch und ökonomisch noch zu aufwendig [ECE97/98].

Micropayments könnten von den *ISP* (Internet Service Provider) oder *IAP* (Internet Access Provider) wirtschaftlich sinnvoll abgewickelt werden. Für die organisatorische Eingliederung der *Nano*- und Micropayments in die Geschäftsprozesse, müßen noch detaillierte Konzepte entwickelt werden.

Neben **Millicent** verfolgen die Systeme PayWord[24] und MiniPay[25] einen erfolgversprechenden Ansatz. Millicent hat, im Vergleich zu den zuletzt genannten Systemen, den entscheidenden Vorteil, daß es bereits kommerziell eingesetzt wird. MiniPay ist bisher nur in geschlossenen Intranets eingesetzt, der Interneteinsatz ist zur Zeit in der Pilotphase [Herz97]. Andere Entwicklungen stellen lediglich ein *Add-On* zu bestehenden Zahlungssystemen dar und erfüllen oft nur unzureichend die speziellen Anforderungen der neuen Zahlungsform, die Geschäftskonzepte in der nahen Zukunft radikal verändern werden.

Die Grenzen zwischen Micropayments und münzorientierten Zahlungssystemen werden verwischen.

Ecash ist zwar eines der weit verbreitetsten *electronic-cash-Systeme*, hat jedoch Einschränkungen, da es z.B. nicht multibankfähig ist. Im Vergleich zu NetCash hat es

[24] http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps

[25] http://www.ibm.net.il/ibm_il/int_lab/mpay

aber die größere Marktdurchdringung und ist deshalb als etabliertes System einzustufen, das sich gegen NetCash durchsetzen wird. Die erfolgreiche Pilotierung des Ecash Systems durch die Deutsche Bank AG erhöht zudem die Relevanz zumindest für den deutschen Online-Markt.

Der entscheidende Vorteil des Ecash ist die optionale Anonymität, die in keinem anderen münzbasierten Konzepts so konsequent verwirklicht wurde. Furche geht davon aus, daß es kein ähnliches System in diesem speziellen Sektor geben wird, solange DigiCash, als Patentinhaber, keine Lizenzen für seine Technologie vergibt.

Die Zukunft wird zeigen welche Systeme sich behaupten werden. Der Trend geht unverkennbar hin zu einem Pool mit einer überschaubaren Anzahl von Zahlungsmitteln, die auf die speziellen Anforderungen abgestimmt sind. Für diesen Pool, mit einem Produktmix aus den beschriebenen Zahlungsmitteln, besteht die Notwendigkeit einer **gemeinsamen Oberfläche und Plattform** ,um eine breite Akzeptanz zu erreichen.

7 Das European Electronic Cash System

Wie das vorangestellte Kapitel zeigte, herrscht besonders im Bereich Zahlungssysteme ein wahrer Wildwuchs von Systemen. Aus den verschiedensten Motivationsgründen heraus wurden in der Vergangenheit Zahlungssysteme entwickelt. Kein einzelnes Modell scheint in absehbarer Zukunft in der Lage zu sein, das Spiel für sich zu entscheiden. Auf lange Sicht werden wahrscheinlich einige Modelle nebeneinander im Internet verwendet werden, denn jeder Anbieter hat seinen eigenen Marktbereich und sein Kundenpotential. [Lyn97]

Das European Electronic Cash System (EECS) ist ein zum Patent[26] vorgelegtes **Geschäftsmodell**, das diese Ausgangssituation nutzt, um eine Dienstleistung daraus abzuleiten und am Markt anzubieten. Das Patent wird in Anhang A dieser Arbeit beigefügt. Für die Konkretisierung der Patentschrift wurden Konzepte dieser Arbeit als Ausgangsbasis verwendet.

In seiner Funktion als Marktmittler [Zbo96] im Bereich Zahlungstransaktions-Abwicklung verfolgt EECS das wesentliche Ziel, Angebots- und Nachfragesegmente an einander anzupassen. Das Angebot an Zahlungsmethoden, das vom Händler oder einer Mall zur Auswahl gestellt wird, soll die tatsächlich vom Käufer nachgefragte Zahlungsmethode enthalten. EECS stellt die Zahlungsmethoden über eine einheitliche Schnittstelle dem Händler oder der Mall, im Sinne einer Querschnittsdienstleistung (vgl. Kap. 2.2), zur Verfügung und übernimmt die Abwicklung der Zahlungen im Auftrag des Händlers.

Die Geschäftsidee von EECS wird im Geschäftsplan von EECS beschrieben.

„Das EECS ... ist ein System, das allen europäischen Verkäufern im Internet, ohne daß diese über eine spezielle Software verfügen, erlaubt, Kreditkarten aller Art und Cybergeld, zu einem späteren Zeitpunkt auch Euroscheckkarte und Geldkarte, anzunehmen. ...Auf das System kann von jeder Internet-Seite ohne spezielle Software zugegriffen werden. Neben seinen Abrechnungsfähigkeiten - es wird nach Anzahl der Buchungen mit den Nutzern abgerechnet - lassen sich für Großkunden spezielle Systeme ... lizensieren.“ [EECS97, S. 2)

EECS nutzt die Intransparenz und Heterogenität des Zahlungssystemmarkts für seine Geschäftstätigkeit und bietet eine intermediäre Funktionalität an.

7.1 Vision

EECS hat es sich zum Ziel gesetzt, ein käuferorientiertes, europaweit einsetzbares Abrechnungssystem zu entwickeln, das möglichst viele, im Internet verfügbare

[26] Für das Verfahren - und das Rechnersystem der EECS besteht unter der Nr. 97110207.4 vorläufiger Patentschutz (Prioritätsschutz) beim Europäischen Patentamt.

Zahlungsmethoden praktikabel bereitstellt, ohne daß der Käufer oder Händler über eine spezielle Software verfügen muß.

Ein käuferorientiertes System zeichnet sich besonders durch die Wahrung der Benutzerinteressen aus (vgl. Kap. 3.2). EECS ist ein von Banken, Netzbetreibern und Zahlungssystemanbietern unabhängiges Unternehmen und hat somit den nötigen Freiheitsgrad, sein Produkt ausschließlich an den Anforderungen der Käufer im Internet auszurichten. Die Begründer von EECS sehen die Ausrichtung ihres Produkts an den **Käuferinteressen** als einen kritischen Erfolgsfaktor an. Die Attraktivität für den Anwender ist entscheidend für den Erfolg eines Produkts im heutigen Wettbewerb der Dienstleistungsanbieter im „Käufermarkt“ Internet.

Der Aspekt eines **europaweit** einsetzbaren Abrechnungssystems bedingt die Mehrsprachigkeit der Anwendung, wie auch die Berücksichtigung der länderspezifischen Gesetzgebung. EECS plant die Zertifizierung seines Systems durch die zuständigen Behörden oder Gremien. Für den deutschen Markt ist hierfür der Zentrale Kreditausschuß (ZKA) zuständig. Die Problematik der Währungsumrechnung wird durch die geplante Einführung des EURO zum 1. Januar 1999 [euro.de] zwar entschärft, bleibt aber grundsätzlich gegeben. Für die europäischen Länder, die nicht oder erst zu einem späteren Zeitpunkt die EG-Währung einführen, und für den globalen Einsatz werden auch in Zukunft Währungskursumrechnungen nötig sein. EECS wird dem Kunden eine Konsolidierung in einer Währung präsentieren.

Das EECS-Abrechnungssystem wird nicht eine weitere proprietäre Zahlungsmethode entwickeln, sondern eine **Kontainerfunktionalität** zur Verfügung stellen, die im Internet eingesetzte Zahlungsmethoden abwickelt. Eine Konkurrenz zu den proprietären Systemen einzelner Banken und Netzbetreibern besteht somit nicht. Es wird vielmehr eine Zusammenarbeit mit diesen Leistungsanbietern im Bereich des Clearings angestrebt. Wie auch bei den beschriebenen Frameworks (vgl. Kap. 6.4) SEMPER und OTP werden die einzelnen Zahlungsmethoden durch in sich geschlossene Kontainer repräsentiert, die mit den anderen Modulen der EECS-Anwendung über definierte Schnittstellen interagieren.

Die Kontainerfunktionalität, die vereinfacht dargestellt die Zahlungsmittel annimmt und verteilt, realisiert den reibungslosen Ablauf der elektronischen Transaktionen zwischen Käufer, Händler und Zahlungssystembetreiber. Durch die serverseitige Bereitstellung des Kontainers kann der Käufer von jeder Webseite, die einen *Link* auf das EECS-System bereitstellt, ohne spezielle Software zugreifen. Dies bedingt den zentralen Ansatz des EECS-Systems, der zusätzlich den inhärenten Vorteil der einfachen Austauschbarkeit bzw. Erweiterbarkeit von Zahlungsmethoden birgt.

Für die Händler bringt dies eine Investitionssicherheit, da Änderungen im Bereich der Zahlungsmethoden von EECS realisiert werden. Den Händlern bleibt der Eigenbetrieb von teuren, technologisch komplizierten Rechnersystemen mit versionsabhängiger, evtl. wartungsintensiver Zahlungssystemsoftware erspart. Die Realisierung der Warenkorbfunktionalität hingegen übernimmt der Händler oder auch eine Mall selbst, als Marktdienst. So kann bei der Produktpräsentation und Bestellannahme bestehender

Gestaltungsspielraum genutzt werden, um die dort vorhandenen Kernkompetenzen und Abgrenzungspotentiale zur Konkurrenz auszubauen.

EECS unterstützt also den Anbieter bei der Implementierung der, an die Erfordernisse des E-Commerce angepaßten, Geschäftsprozesse im Bereich Zahlungssysteme. Für den Händler resultiert hieraus die effektive Implementierung der E-Commerce-Strategien, im Einklang mit neuen und bestehenden Geschäftsmodellen, was als Schlüssel für den zukünftigen Unternehmenserfolg im Internet gesehen werden kann [Kam97].

Für eine Mall kann EECS die Querschnittsdienstleistung Zahlungsabwicklung vollständig übernehmen, oder aber die Software in Lizenz zur Verfügung stellen. EECS ermöglicht die Abrechnung von *Multimandanten-Zahlungen* und verteilt die vom Käufer, in einer Transaktion bezahlten Sammelbeträge, an die entsprechenden Händler respektive Mandanten. Wartung, Kundendienst und Call-Center-Funktionen kann EECS für die Mall übernehmen.

7.2 Transaktion

„*Jede Transaktion ist ein Austausch.... Man kann Güter oder Dienste gegen Geld austauschen oder auf der Basis des Tauschhandels. Im technischen Sinne besteht eine Transaktion aus einer Reihe von Schritten, die durchgeführt werden müssen, um einen Austausch zu erreichen, insbesondere bei einer elektronischen Transaktion*“. [Lyn97]

Die EECS-Transaktion setzt sich aus mehreren Teiltransaktionen zusammen, die nacheinander ablaufen. Wie in Abbildung 7-1 dargestellt wird zunächst durch anklicken des ◎ „EECS-Bezahl-Knopfs“ in der Händlerapplikation eine **Transaktionsanfrage** übermittelt. Der Transaktionsanfrage wird ein eindeutiger Identifikationscode (eine Transaktions_ID) vergeben und über ein *Java-Applet* wird im Browser des Käufers ein **Zahlungsformular** in dessen Landessprache generiert.

Anhand der im Zahlungsformular ausgewählten Alternativen, die mit den Händlerpräferenzen abgeglichen werden, erfolgt die Verarbeitung der **Zahlungstransaktion**. Die entsprechend der Geschäftsprozess-Beschreibung (vgl. Kap. 7.4) definierten Abläufe werden abhängig von der ausgewählten Zahlungsmethode durchlaufen, Zusatzfunktionen wie z.B. Schlüsselgenerierung, Autorisierung, etc. werden ausgeführt. Kann die Zahlungstransaktion fehlerfrei abgearbeitet werden und erfolgt eine Zahlungsbestätigung, erhalten Käufer und Händler eine positive Transaktionsbestätigung und der **Transaktionsabschluß** wird durchgeführt. Wird die Zahlungstransaktion nicht erfolgreich durchlaufen, erhalten Käufer und Händler eine negative Transaktionsbestätigung und die Zahlungstransaktion wird zurückgesetzt.

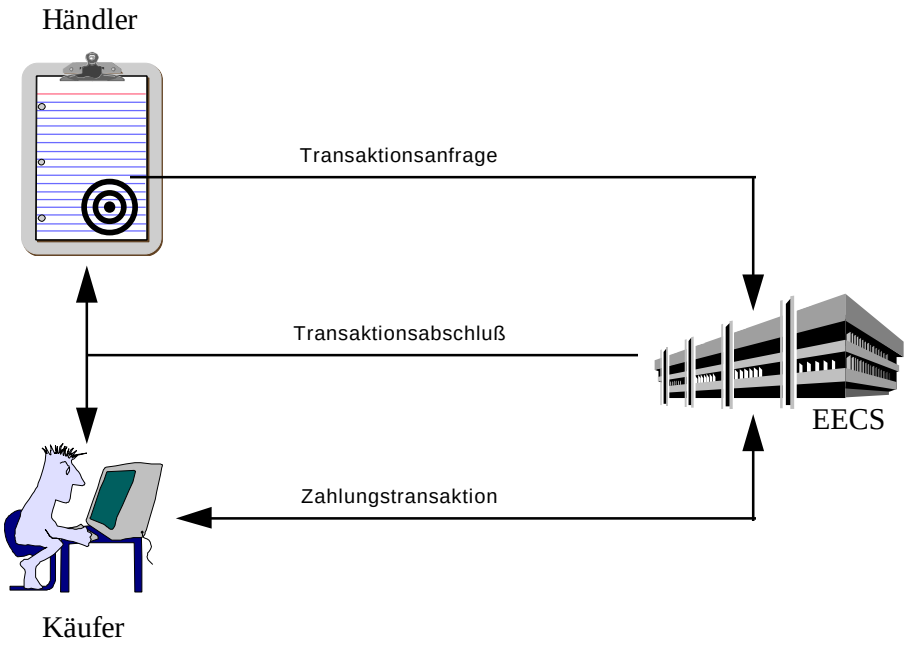


Abbildung 7-1; EECS-Transaktion

Der Transaktionsstatus (Transaktions_stat) gibt zu jedem Zeitpunkt Auskunft darüber, in welcher Phase bzw. in welchem Zustand sich die Transaktion befindet.

7.3 Funktionalität

Nachfolgend wird der geplante Leistungsumfang der EECS-Applikation beschrieben [EECS97]. Eine grundsätzliche Einteilung der Bereiche erfolgt über deren Bezug zu den *Entitäten* des Systems. Wir unterscheiden die **Bereiche:**

- Händler
- Transaktionsabwicklung
- Transaktionshistorie
- Ultimoabrechnung
- Netzverwaltung

Innerhalb dieser Bereiche lassen sich Funktionen identifizieren, die durch die spezifischen Anforderungen an das System geprägt sind. Die nachfolgenden Tabellen geben einen Überblick über die Funktionen und deren Ausprägungen innerhalb der Bereiche.

7.3.1 Händler

Der Bereich Händler repräsentiert die Funktionen, die für den Händler relevant sind. Es werden unter anderem die Pflege der Stammdaten, mit den individuellen Präferenzen, und Funktionen zur Informations- bzw. Auskunftserstellung abgedeckt. Die Präferenzdaten des Händlers ermöglichen ein individuelles *Customizing* des Systems durch den Händler selbst mittels Parameter. Zudem soll ein Testsystem für Interessenten, die das System zunächst einmal zur Probe auf ihrer Webseite anbieten, realisiert werden.

Funktion	Ausprägung
Händler-Kundenstamm	• *Händler anlegen* • *Händler verwalten* • *Händler löschen* • *Händler sperren*
Händlerpräferenzen	• *Transaktionspräferenz* ⇒ Freigabe Zahlungsmethoden ⇒ Sprachvarianten ⇒ Formulargestaltung • *Abrechnungspräferenz* ⇒ Gebührenstruktur ⇒ Kommunikationsvarianten / -pfade
Händler-Konten-Abfrage[27]	• *transaktionsbezogen* • *abrechnungsbezogen*
Händler-Testsystem	• *E-Mail Anfrage des Interessenten bearbeiten* • *Interessenten Bewertung* • *automatische Übernahme von Interessenten als Händler nach x Tagen*

[27] Authentisierung über eine spezielle, individuelle Bewegung der Maus, die sogenannte Geste

7.3.2 Transaktionsabwicklung

Im Bereich Transaktionsabwicklung werden die Funktionen beschrieben, die für eine reibungslose und komfortable Transaktionsabwicklung benötigt werden. Hierbei wird die Käufer- aber auch die Händlerschnittstelle näher spezifiziert, sowie die Kontainer mit den Zahlungsmethoden.

Funktion	Ausprägung
Käuferinterface[28]	• *Zahlungsinitiierung* • *Schlüsselgenerierung* • *Autorisierung* • *Transaktionsbestätigung* (E-Mail oder direct write)
Händlerinterface	• *Übernahme zahlungsrelevanter Bestelldaten* • *Abgleich Händler-Präferenzdatei* • *Zahlungsbestätigung*
Zahlungsmethoden	• *SET-Protokoll* • *E-cash* • *NetBill* • *HBCI-Protokoll* ⇒ electronic direct debit ⇒ electronic cash ⇒ GeldKarte • *Millicent*
Transaktionsabschluß	• *Datenübergabe an Transaktionshistorie* • *Datenübergabe an Abrechnungsdaten*

[28] Die Sprachvariante wird in Abhängigkeit der Käufernationalität ausgewählt

7.3.3 Transaktionshistorie

Die Transaktionshistorie umfaßt alle beschreibenden Daten des Systems zu einem Zeitpunkt. Sie dient als Basis für die Call-Center-Aktivitäten, aber auch als Schnittstelle zur Finanzbuchhaltung und enthält alle abgeschlossenen Transaktionen des letzten Zeitintervalls. Die Daten werden, wie dies auch im Bankverkehr üblich ist, für einige Zeit gespeichert, um eventuell auftretende Konflikte klären zu können, danach werden sie gelöscht.

Funktion	Ausprägung
Datenübernahme	• *abgeschlossene Transaktionen* • *aus Ultimoabrechnung* • *aus FIBU*
Call-Center-Funktion	• *Auskunft* ⇒ E-Mail ⇒ phone • *Änderungsauftrag* ⇒ Abgleich mit Händlerdaten / EECS-Daten ⇒ Vorgang an Verantwortlichen weiterleiten (Gutschrift, Rückzahlung, Korrektur, etc.) ⇒ Bestätigung Änderungauftrag • *Protokoll für Statistik*
Statistische Auswertungen	• *Ad-hoc-Queries* • *periodische Auswertungen*
Archivierung	• *Bestand und Protokolle*

7.3.4 Ultimoabrechnung

Die Ultimoabrechnung wird zu einem Zeitpunkt X durchgeführt. Sie veranlaßt alle notwendigen Umbuchungen, Gebührenermittlungen und Rechnungsstellung etc.

Funktion	Ausprägung
Umbuchungen	• *Aggregation* • *Währung* ⇒ Währungs-Unterkonten ⇒ Währungs-Tageskurs-Pflege ⇒ Währungsumrechnung • *Buchungsinitiierung* ⇒ Bank ⇒ FIBU
Buchungsgebühren	• *Gebührenstaffel* • *Gebührenermittlung*
Fakturierung	• *Händler* • *Datentransfer FIBU*
manuelle Änderungsmöglichkeiten	• *Gutschrift* • *Storno*
Schnittstelle zur Finanzbuchhaltung	• *Zahlungskontrolle* ⇒ Zahlungseingang ⇒ Mahnwesen • *Rückmeldung an Transaktionshistorie*

7.3.5 Netzverwaltung

Als ein separater Bereich wird die Netzverwaltung und deren Funktionalität beschrieben. Das sicherheitskritische Rechnernetz und die Netzverbindungen nach Außen (Internet, Clearingnetze der Banken) stellen besonders hohe funktionale Sicherheitsanforderungen.

Funktion	Ausprägung
Ressourcenverwaltung	• *Webserver* • *Protokollrechner zu den Clearingstellen*
Protokollierung	• *Intrusion Detection System* [Löh98] • *Verhaltens-Profiling*
Neustart	• *Aufsetzpunkt* • *Startskript* • *DB-Recovery*

7.4 Geschäftsprozesse

Innerhalb dieses Kapitels sollen die Prozesse als Szenario beschrieben werden, die durch das Aktivieren des ◎ *„Bezahl-Knopfs“* innerhalb der EECS-Applikation angestoßen werden. Der ◎ *Bezahl-Knopf* repräsentiert den Link auf der Händler-Webseite, der die Verbindung zu EECS herstellt (vgl. Abbildung 7-1).

Die Auswahl der Systeme, für die ein EECS-Geschäftsprozess definiert wurde, berücksichtigt die in Kapitel 6 beschriebenen Zahlungsmethoden. Es wird jeweils ein System exemplarisch für die unterschiedlichen Kategorien bearbeitet.

In der nachfolgend modellierten Version des EECS-Systems haben also Käufer und Händler die freie Auswahl zwischen den Systemen:

- SET-basierte Zahlung
- Ecash
- NetBill
- HBCI-basierte Überweisungskopie
- Millicent

Auf Grund der Informationspolitik einiger Zahlungssystemanbieter, wie z.B. CyberCash oder T-Online, die ihre Message-Formate nicht offenlegen, konnten interessante und

vielversprechende Lösungsansätze nicht berücksichtigt werden. Diese Arbeit beschränkt sich auf Systeme, die zur Zeit dokumentiert und veröffentlicht sind.

Für die Darstellung der Geschäftsprozesse, in den Abschnitten 7.4.2 bis 7.4.6 dieser Arbeit, wird die Notation des Interaktionsdiagramms nach Rumbough [Rum93] verwendet.

7.4.1 Allgemeine Komponenten der Geschäftsprozesse

Ist die Kaufentscheidung gefallen, und der Käufer hat die Zahlungstransaktion durch anklicken des ◎ „*EECS-Bezahl-Knopf*“ initiiert, werden verschiedene Parameter ausgewertet, um die Präferenzen der Transaktionspartner in Einklang zu bringen, und so die Zahlungstransaktion aus Sicht des Käufers und der Händler ökonomisch, komfortabel und sicher abzuwickeln (vgl. Kap 7.3.1 und Kap. 7.3.2).

Der **Händler** kann seine **Präferenzen wählen**:

- Grundsätzlich akzeptierte Zahlungssysteme
- Bonität des Kunden (falls nicht anonym)
- Zahlungsmodell (pre-paid, pay-now, post-paid)
- Auswahl des Zahlungssystems in Abhängigkeit vom verkauften Produkt und der Transaktionsparameter
    - digitale bzw. physische Güter
    - Rechnungsbetrag
    - Ort bzw. Land der Liefer- oder Rechnungsadresse
    - Grad der Geschäftsbeziehung (etabliert versus neu)
- Oberes und unteres Betragslimit je Zahlungssystem
- Sicherheitslevel
- Zuverlässigkeit und Verfügbarkeit des Systems
- Anfallende Transaktionskosten

Der **Käufer** wählt seine **Präferenzen:**

- Grundsätzlich verfügbare Zahlungssysteme
- Oberes und unteres Betragslimit je Zahlungssystem
- Zahlungsmodell (pre-paid, pay-now, post-paid)
- Seriosität des Anbieters
- Anonymität
- Sicherheitslevel
- Zuverlässigkeit und Verfügbarkeit des Systems
- Anfallende Transaktionskosten

7.4.2 Geschäftsprozess HBCI

HBCI ist von seiner ursprünglichen Ausrichtung her schlecht geeignet über einen Dienstleister, der zusätzlich zu Bankkunde und Kreditinstitut auftritt, abgewickelt zu werden. Dagegen spricht zum einen das enge Vertrauensverhältnis zwischen Kunde und Kreditinstitut und zum anderen die eher restriktiven Vertragsverhältnisse zwischen den Partnern, die zwar Garanten für das entgegengebrachte Vertrauen sind, jedoch wenig Freiraum für geänderte Geschäftsprozessketten lassen.

Angesichts der Popularität der Bezahlform „Überweisung“ und des enormen Potentials an Transaktionen über die EC-Karte und die GeldKarte kann davon ausgegangen werden, daß das HBCI-Modell des Geldtransfers online zugänglich gemacht wird. HBCI wäre dann möglicher Nachfolger des klassischen Datenträgeraustausches (DTA[29]). Das HBCI-Protokoll ist nicht nur für Homebanking, sondern auch als Variante im Szenario der elektronischen Zahlungssysteme geeignet.

In Deutschland, wie auch im übrigen Europa, wird ein Großteil der Transaktionen über das Girosystem abgewickelt. Berücksichtigt man dies bei der Gestaltung des Geschäftsprozesses, so wäre zum jetzigen Zeitpunkt eine sinnvolle Einbindung in die EECS-Abrechnung über einen Feedback-Mechanismus z.B. eine Überweisungskopie möglich. Das Ziel elektronischer Zahlungssysteme, eine rasche und überprüfbare Zahlung zwischen Käufer und Händler bereitzustellen, wäre ein Stück weit erreicht [Stol97]. Durch einen nachweislich erfolgten Online-Überweisungsauftrag hätte der Händler zumindest die Garantie, daß die Überweisung sofort zur Bank gesendet wurde und nicht noch einige Tage „Liegezeit“ beim Zahlungspflichtigen hat. Allerdings trägt der Händler das Risiko, daß seine Rechnung nicht beglichen wird, da der erteilte Überweisungsauftrag vom Kunde widerrufen werden kann, oder die Bank den Auftrag nur bei vorliegender Deckung ausführt.

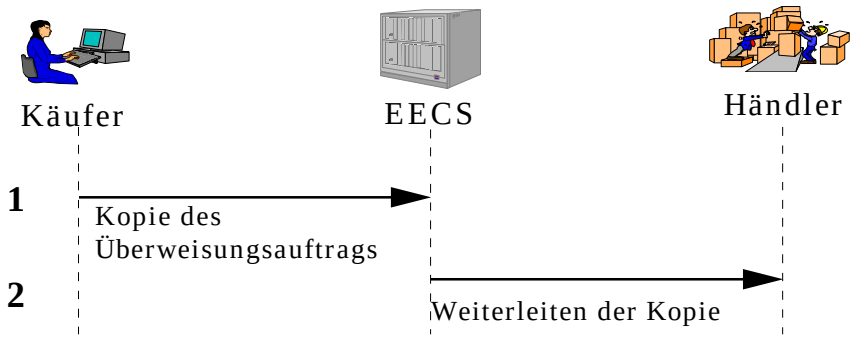


Abbildung 7-2; Geschäftsprozess HBCI

1. Der Käufer erstellt und versendet über seine Homebanking-Applikation einen Überweisungsauftrag und schickt eine **Kopie** an EECS.
2. EECS leitet diese Kopie an den Händler weiter.

[29] „Im beleglosen Datenträgeraustausch nimmt das Kreditinstitut Aufträge für Überweisungen und Lastschriften auf Datenträgern entgegen.“ [CODAT96]

7.4.3 Geschäftsprozess SET

Die SET-Message-Struktur legt Anfrage/Antwort-Message-Paare fest, die in einem maschinenunabhängigen Format definiert sind. Dieses Format ermöglicht die Verarbeitung der Anfragen auf verschiedensten Servern. Die Verschlüsselung wird auf Teilbereiche der Daten angewandt, so daß eine partielle Entschlüsselung der Nachricht, je nach dem Informationsbedarf bzw. Datenschutzbedürfniss vorgenommen werden kann. Bei einer Verschlüsselungsmethode über die gesamte Nachricht könnte eine solche Funktionalität nicht implementiert werden.

Das Zertifikatsmanagement, das ein wesentlicher Bestandteil des SET-Konzepts ist, wird in dieser Arbeit nicht detailliert erörtert, vielmehr wird auf die Ergebnisse der Arbeit von Pfeffer [Pfef96] aufgebaut und verwiesen.

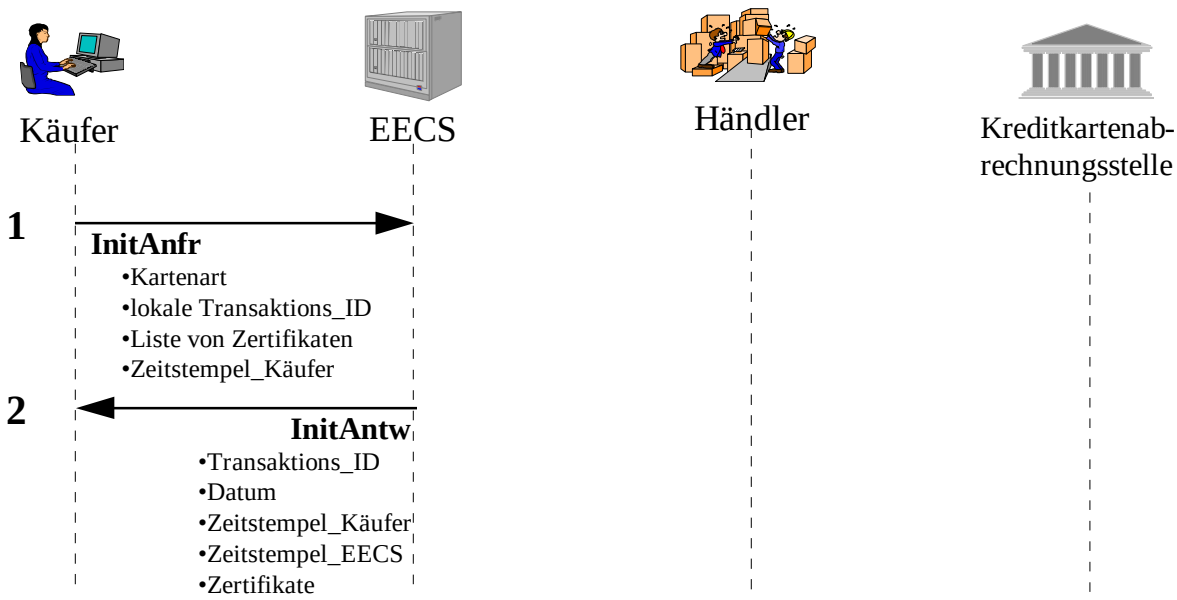


Abbildung 7-3; SET Geschäftsprozess - Initialisierungsphase

1. Initialisierungsanfrage (**InitAnfr**)
   Die *InitAnfr* wird vom Käufer geschickt, wenn dieser bereit ist die im Bestellformular aufgelisteten Waren zu den angegebenen Bedingungen zu bezahlen.
   Dateninhalt der *InitAnfr* ist:
   Kartenart (Visa, Mastercard, etc.); lokale ID der Transaktion; Liste von Zertifikaten; Zeitstempel_Käufer (eine Variable zur Überprüfung der Aktualität).

2. Dateninhalt der Initialisierungsantwort (**InitAntw**) ist:
   Transaktions_ID (generiert aus der lokalen ID der Transaktion, der InitAnfr und einer globalen eindeutigen ID); Datum; Zeitstempel_Käufer; Zeitstempel_EECS; Zertifikate mit den vom Käufer benötigten Schlüsseln.

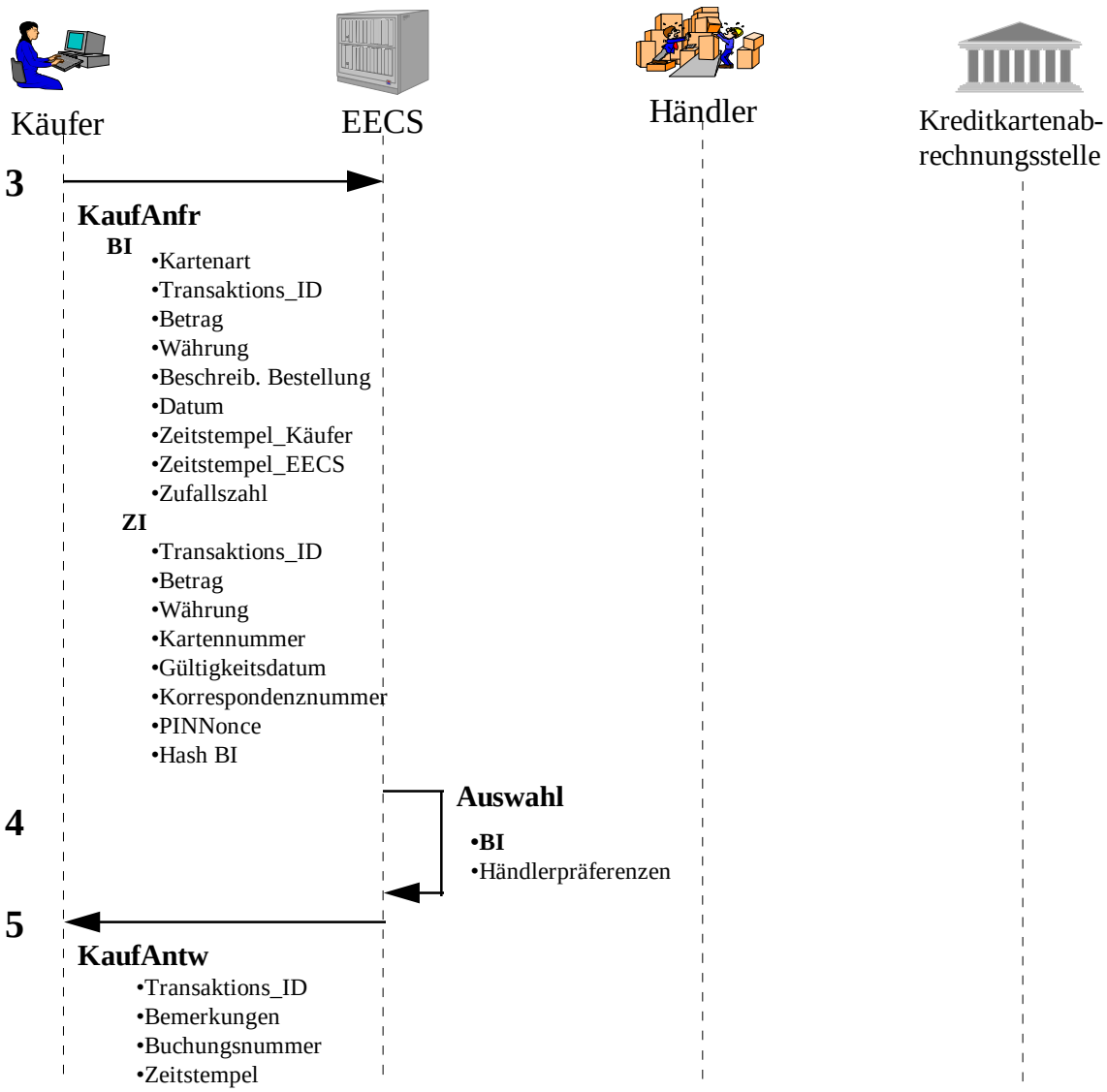


Abbildung 7-4; SET Geschäftsprozess - Kaufphase

3. Die Kaufanfrage (**KaufAnfr**) besteht aus der Bestellinformation (**BI**) und der Zahlungsinformation (**ZI**).
   Die *BI* enthält Daten aus der Initialisierungsphase, Betrag, Währung, Datum und Beschreibung der Bestellung. Aus dem Hashwert der *BI* und dem Hashwert der *ZI* wird eine duale Signatur erzeugt. Diese duale Signatur wurde im SET Standard optimiert, so daß nur ein Originaldatenpaket erstellt werden muß, das an Händler und Kartenabrechnungssgesellschaft gesandt wird und nur die jeweils relevanten Informationen entschlüsselt werden können. Die *ZI* ist mit dem public-key der Kartenabrechnungssgesellschaft verschlüsselt, so daß weder Händler noch EECS diese lesen kann. Sie wird nur bei der Autorisierung weitergeleitet. Hierfür wird die normale DES 56-bit Verschlüsselung oder die stärkere RSA 1024-bit Verschlüsselung eingesetzt. Die *ZI*-Daten setzen sich zusammen aus den verschlüsselten Kartendaten: Kartennummer, Gültigkeitsdatum, Korrespondenznummer, PINNonce, sowie Transaktions ID, Betrag und einem Bestell-

Hashwert. Diese *ZI*-Daten zusammen mit der dualen Signatur stellen die *ZI* dar, die wiederum mit dem privaten Schlüssel des Käufers verschlüsselt werden.

4. Wenn EECS die KaufAnfr erhält, extrahiert sie zunächst die *ZI* und *BI*, um die duale Signatur der ***BI*** mit Hilfe des Zertifikats zu verifizieren. Der Abgleich der *BI* mit den Händlerpräferenzen gibt Aufschluß über den weiteren Prozessablauf.

5. Hat der Händler in seiner Präferenzdatei z. B. für kleinere Beträge keine Autorisierungsprüfung vorgesehen, wird nun die ***KaufAntw*** erstellt. Folgt eine 'nur Autorisierung' weist die *KaufAntw* den Käufer an, zu einem späteren Zeitpunkt den Transaktionsstatus zu erfragen (vgl. 10. *InhabAnfr*), oder es folgt die Autorisierung (vgl. 6. *AutAnfr*) und der Zahlungsauftrag (vgl. 8. *ZahlAnfr*).

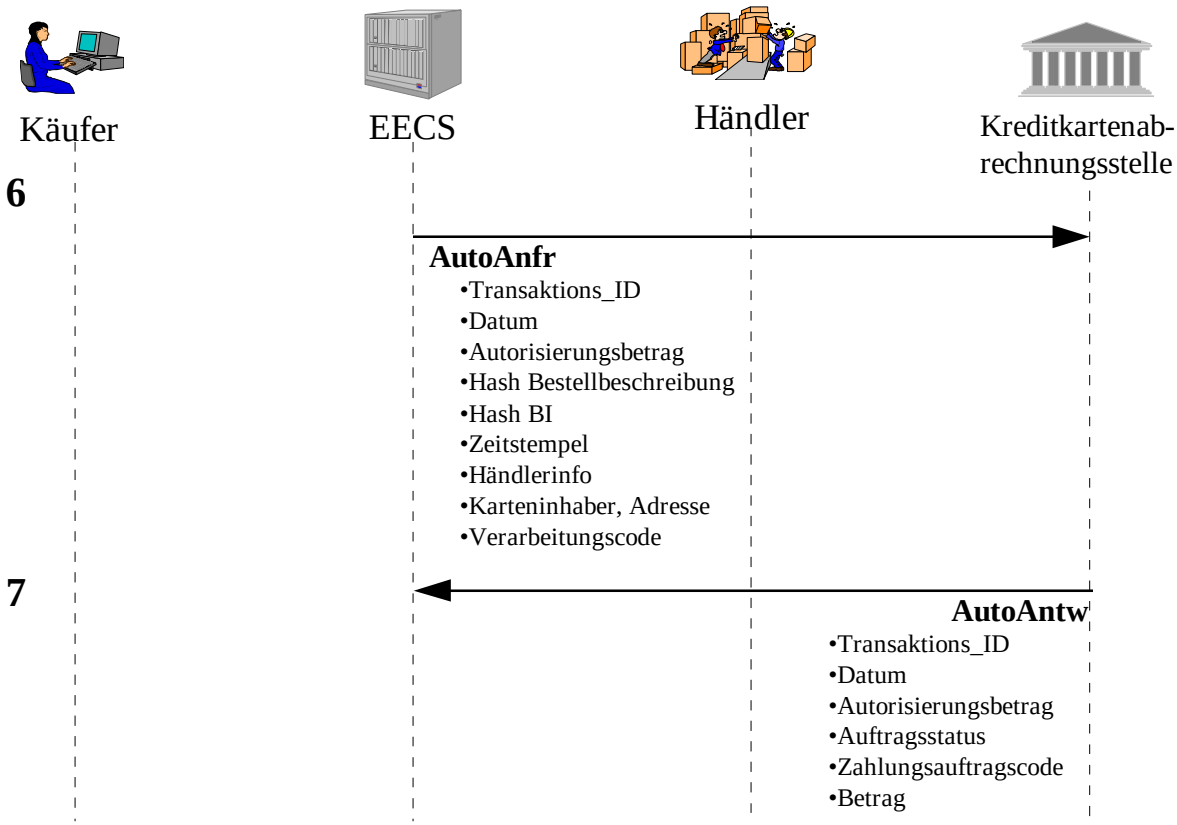


Abbildung 7-5; SET Geschäftsprozess - Autorisierung

6. Die Autorisierung sichert dem Händler die Kreditwürdigkeit des Karteninhabers zu und bemächtigt ihn den Transaktionsbetrag einzuziehen. Die Autorisierungsanfrage (***AutoAnfr***) beinhaltet unter anderem den Bestell-Hashwert, anhand dessen die Übereinstimmung von Händler_Bestellinfo und Käufer_Bestellinfo geprüft werden kann, den *BI*-Hashwert, der sicherstellt, daß der Karteninhaber für genau diese Bestellung die *ZI* zur Verfügung gestellt hat, Rechnungsadresse des Karteninhabers, Branche des Händlers, etc., sowie die Angabe über den Verarbeitungscode (nur Autorisierung, Autorisierung und Zahlungsauftrag)

7. Die Kartenabrechnungsgesellschaft prüft die gesendeten Angaben und erhält eine positive Autorisierung mit einem Auftragsstatus (capture token), oder den

Sperrvermerk. Die ***AutAntw*** beinhaltet je nach Autorisierungsbetrag, den Auftragsstatus oder den Zahlungsauftragscode und den Betrag. In beiden Fällen kann davon ausgegangen werden, daß die Ware bezahlt wird.

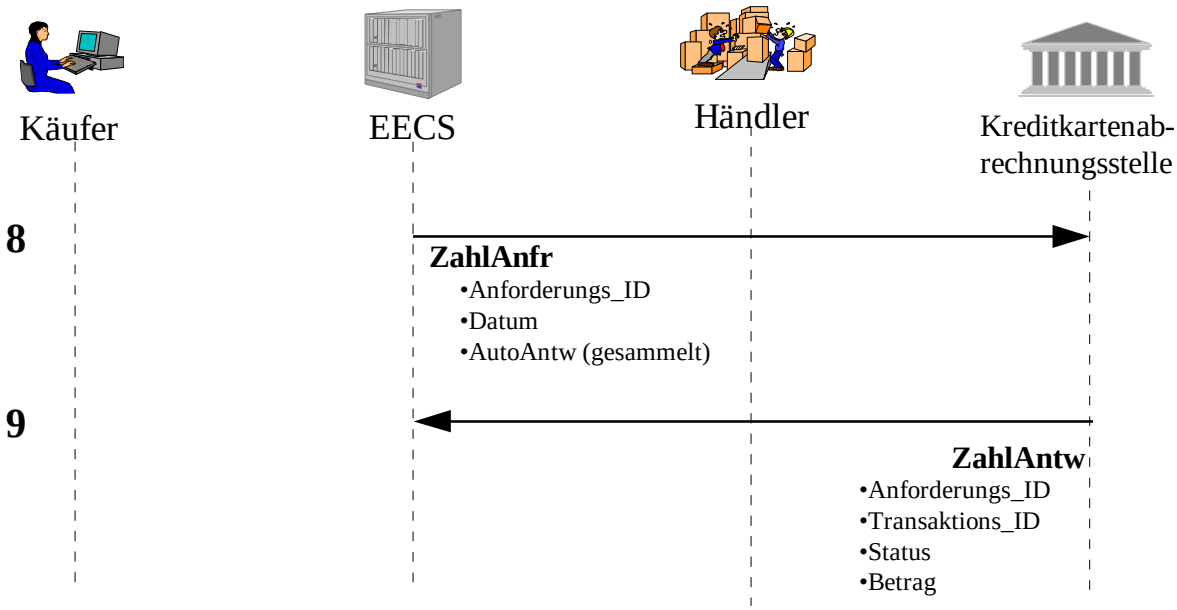


Abbildung 7-6; SET Geschäftsprozess - Zahlungsphase

8. EECS schickt den Zahlungsauftrag bzw. ***ZahlAnfr*** an die Kreditkartenabrechnungsstelle, die diesen über ihr Clearingnetzwerk abwickelt. Dies kann simultan zu den Kauftransaktionen geschehen, oder EECS sammelt die *AutoAntw* der verschiedenen Transaktionen und schickt diese z. B. am Tagesende als Batch an die Abrechnungsstelle.

9. Zu diesem Zeitpunkt werden die Gebühren für die Transaktion von der Abrechnungsstelle belastet, bzw. der Gutschriftsbetrag wird um den Gebührenbetrag vermindert. EECS erhält die ***ZahlAntw*** vom Zahlungsgateway und veranlaßt, falls dies noch nicht geschehen ist, eine *KaufAntw* an den Karteninhaber (vgl. 5. *KaufAntw*).

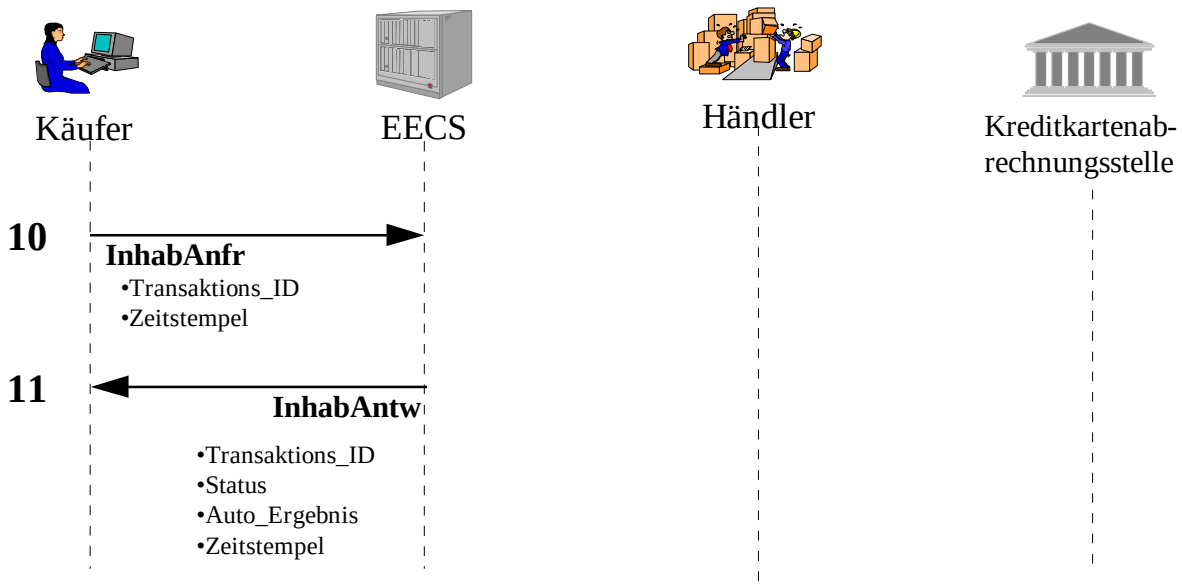


Abbildung 7-7; SET Geschäftsprozess - Inhaberanfrage

10. Der Karteninhaber kann jederzeit über eine Inhaberanfrage (***InhabAnfr***) den Transaktionsstatus der Zahlungsabwicklung abfragen. Hierzu schickt er die Transaktions-ID und einen Zeitstempel an EECS.
11. EECS antwortet mit der Inhaberantwort (***InhabAntw***) in der Form: Transaktions_ID, Status, Ergebnisse der Autorisierung und Zeitstempel.

7.4.4 Geschäftsprozess Ecash

Bei einem Einkauf kann der Kunde mit seinen im Wallet gespeicherten Ecash-Münzen bezahlen. Die Protokolle, die für die Produktauswahl und Bestellabwicklung benötigt werden, sind nicht Gegenstand der Ecash-Spezifikation.

Entscheidet der Kunde, zu zahlen, wird der Betrag vom Wallet des Kunden eingezogen. Da ein Wechselvorgang die Anonymität des Ecash-Besitzers aufheben würde, wird der exakte Betrag vom Wallet eingezogen.

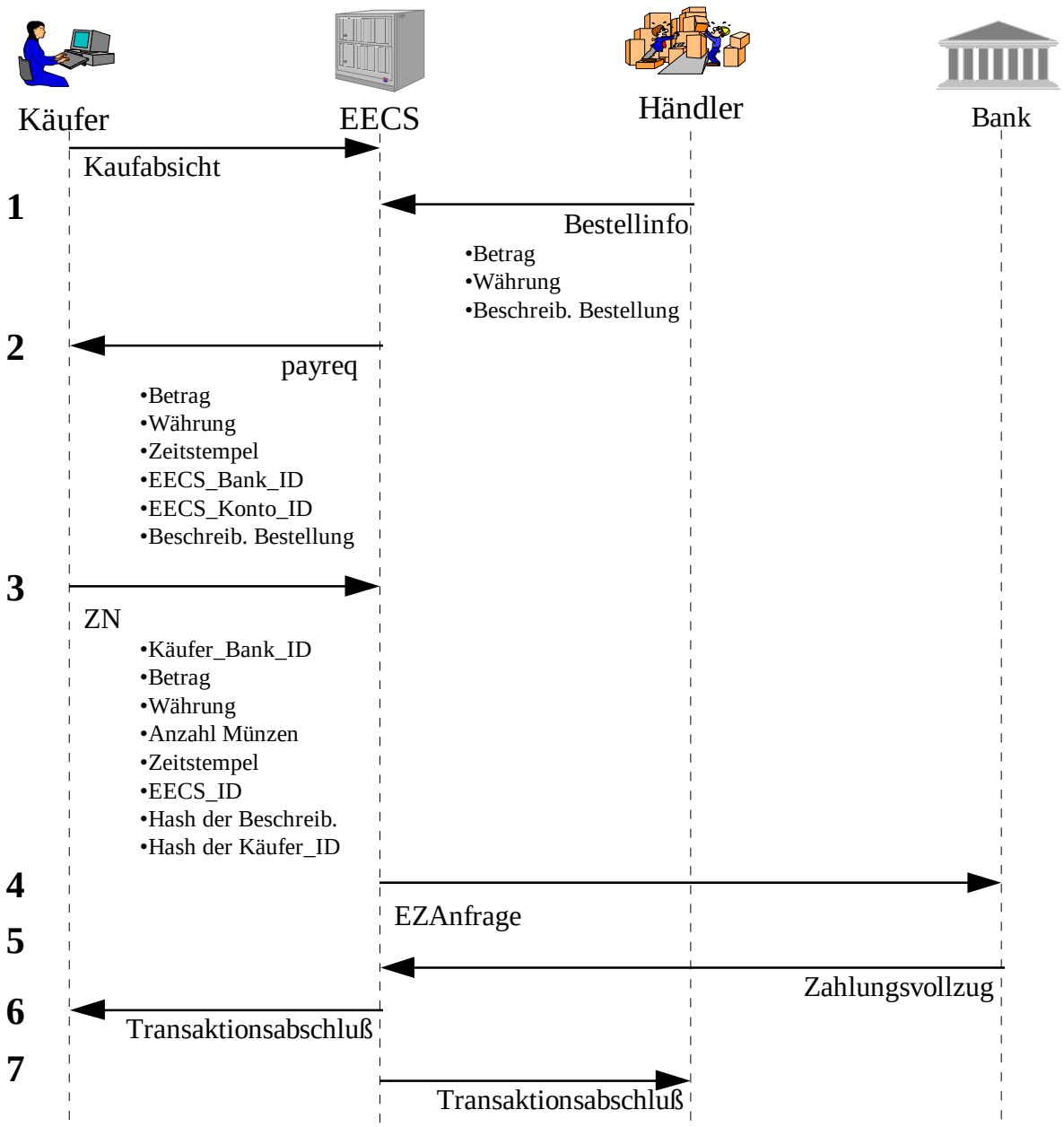


Abbildung 7-8; Geschäftsprozess Ecash

1. EECS fordert von den Händlern die zahlungsrelevanten Bestellinformationen an und generiert eine Zahlungsaufforderung (***payreq***). Diese *payreq* enthält Betrag, Währung, Zeitstempel, EECS_Bank_ID, EECS_Konto_ID und Beschreibung der Bestellung.
2. Die *payreq* wird an das Wallet des Käufers geschickt. Das Käufer-Wallet bereitet diese Informationen auf und der Käufer wird aufgefordert, die Zahlung zu bestätigen. Es wird eine Zahlungsnachricht (***ZN***) generiert in der Form:

   $$ZN = [ZI,[Münzen,H(ZI)]PK_{Bank}]$$

   wobei *ZI* die Zahlungsinformationen Käufer_Bank_ID, Betrag, Währung, Anzahl

Münzen, Zeitstempel, EECS_ID, Hashwert der Beschreibung und Hashwert der Käufer_ID enthalten.

3. Der Käufer schickt die *ZN* an EECS.
4. EECS muß nun die erhaltenen Münzen in ihrem Depot bei der Ecash Bank einlagern. Sie erstellt eine Einzahlungsanfrage (***EZAnfrage***):

   $$EZAnf = [[ZN]Sig_{EECS}]PK_{Bank}$$

   und schickt diese an die Bank.
5. Die Ecash Bank entschlüsselt und prüft die Münzen anhand der Seriennummern in ihrer Datenbank. Wird das Ecash von der Bank akzeptiert, schreibt diese den Betrag auf dem EECS-Konto gut und schickt eine Nachricht über den ***Zahlungsvollzug***.
6. EECS schickt an den Käufer die Meldung über den erfolgreichen ***Transaktionsabschluß***.
7. EECS schickt an die Händler die Meldung über den erfolgreichen ***Transaktionsabschluß***.

7.4.5 Geschäftsprozess NetBill

NetBill nutzt ein modifiziertes Kerberos-Schema [KoN93] für die Authentifizierung. Das Ziel der Modifizierung ist die Beibehaltung der effizienten symmetrischen Verschlüsselung für den Großteil der Informationen bei gleichzeitiger Verringerung der Abhängigkeit vom Server. Dies wird dadurch erreicht, daß der öffentliche Schlüssel in Teilen des Protokollaustauschs benutzt wird. Das daraus entstandene Protokoll heißt Public Key Kerberos.

Im traditionellen Kerberos, wenn A mit B kommunizieren will, muß zunächst ein Ticket (T_{AB}) bei einem speziellen Anwendungsserver und ein Schlüssel (K_{AB}) beschafft werden. Nun sendet A

$$T_{AB},K_{AB}[Nachricht]$$

B kann K_{AB} aus dieser Nachricht extrahieren und die Nachricht entschlüsseln. Die Nachricht war vor dem Abhören gesichert und A konnte eindeutig identifiziert werden.

Im NetBill Schema erhält A sein Ticket direkt von B, in der Form

$$K_{OneTime}[A,B,TimeStamp,K_{Challange}],PK_B[K_{OneTime}],Sig_A$$

wobei $K_{OneTime}$ für einen Einmalschlüssel und $K_{challange}$ für irgendeinen symmetrischen Schlüssel steht. Voraussetzung für die Entschlüsselung der Nachricht ist, daß A und B Zugriff auf den öffentlichen Schlüssel des Anderen haben. B setzt seinen privaten Schlüssel ein, um $K_{OneTime}$ zu entschlüsseln und Zugriff auf $K_{challange}$ zu erhalten. B konstruiert nun ein Kerberos Ticket und sendet es an A, mit den Daten

$$K_{Challange}[T_{AB},K_{AB}]$$

A dechiffriert die Nachricht um T_{AB} und K_{AB} im Klartext zu erhalten, und weiß somit, daß die Nachricht von B generiert wurde.

Bevor eine NetBill-Transaktion stattfindet, wird in der oben beschriebenen Weise ein T_{CM} mit Käufer und EECS, sowie ein T_{MN} mit EECS und dem NetBill-Server und ein T_{CN} mit Käufer und dem NetBill-Server vereinbart. Die Gültigkeitsdauer der Tickets ist konfigurierbar, überspannt aber normalerweise den Zeitraum einiger Transaktionen.

Das Transaktionsprotokoll von NetBill untergliedert sich in drei Phasen:

Angebotsphase:

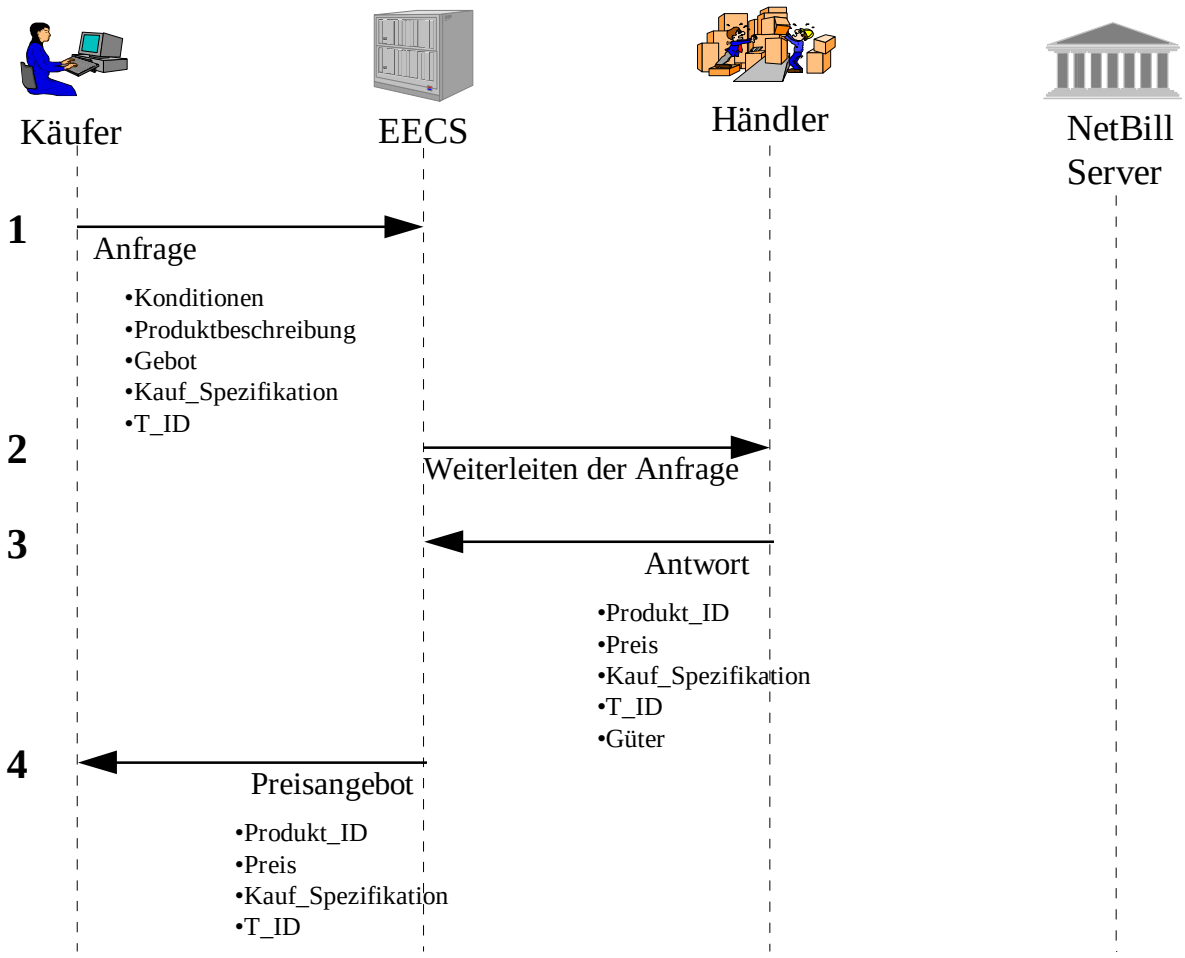


Abbildung 7-7; Geschäftsprozess NetBill - Angebotsphase

1. Der Käufer schickt zunächst seine **Anfrage** in der Form:

$$T_{CM},K_{CM}[\text{Konditionen,Produktbeschreibung,Gebot,Kauf\_Spezifikation,T\_ID}]$$

EECS extrahiert K_{CM} aus dem Ticket und dechiffriert die Anfrage, die im einzelnen aus den Konditionen (Ausweis über den Anspruch auf besondere Preisvergünstigungen), Produktbeschreibung (product request data - PRD), Kauf_spezifikation (nähere Spezifikation des Kaufs) und der T_ID (eindeutige Transaktions ID) besteht.

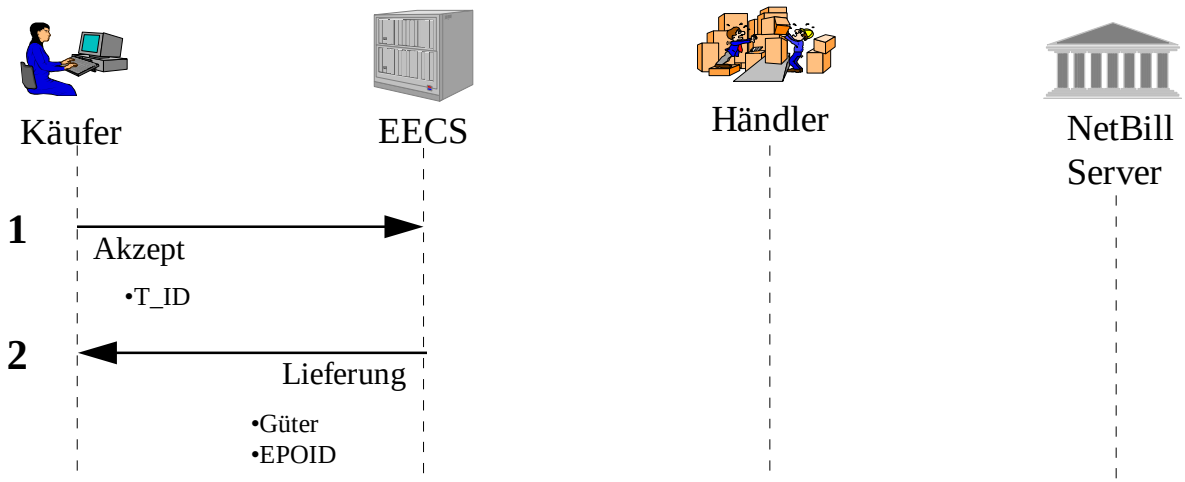
2. EECS leitet die zuvor dechiffrierte Anfrage an den Händler weiter.
3. Der Händler generiert auf Grund dieser Daten eine **Antwort** für EECS mit dem Preisangebot und schickt es zusammen mit den Gütern, bzw. Produkten als Dokumente oder Dateien an EECS.
4. EECS separiert die Güter, speichert sie zwischen und unterbreitet das **Preisangebot** dem Käufer in der Form:

   K_{CM}[Produkt_ID,Preis,Kauf_Spezifikation,T_ID]

   T_ID stellt die Verbindung zu der ursprünglichen Anfrage her. Die Produkt_ID ist eine textuelle Beschreibung des Produkts.

Die Verhandlungen über den Preis und die Konditionen kann noch einige der oben beschriebenen Anfrage/Antwort Kommunikationen durchlaufen, bevor der Käufer sich zum Einkauf entscheidet und die Warenlieferungsphase initiiert.

Warenlieferungsphase:



1. Der Käufer akzeptiert das Angebot, indem er die Nachricht

   T_{CM},K_{CM}[T_ID]

   als **Akzept** sendet.
2. EECS **liefert**, indem sie einen Zufallsschlüssel KGoods generiert, der zur Verschlüsselung der gelieferten Informationen genutzt wird und versendet das chiffrierte Produkt an den Käufer im Format:

KGoods[Güter],KCM[SHA[KGoods[Güter]]],EPOID

Der Käufer kann die Richtigkeit der gelieferten Informationen (Güter) prüfen, indem er den SHA Algorithmus auf *KGoods[Güter]* anwendet und diesen Wert mit dem von EECS erzeugten, mitgelieferten Wert auf Übereinstimmung vergleicht. Die *EPOID* (electronic payment order ID) wird benötigt um diese Transaktion in der NetBill Datenbank eindeutig zu identifizieren. Sie enthält Informationen über EECS und Zeitstempel etc.

Zahlungsphase:

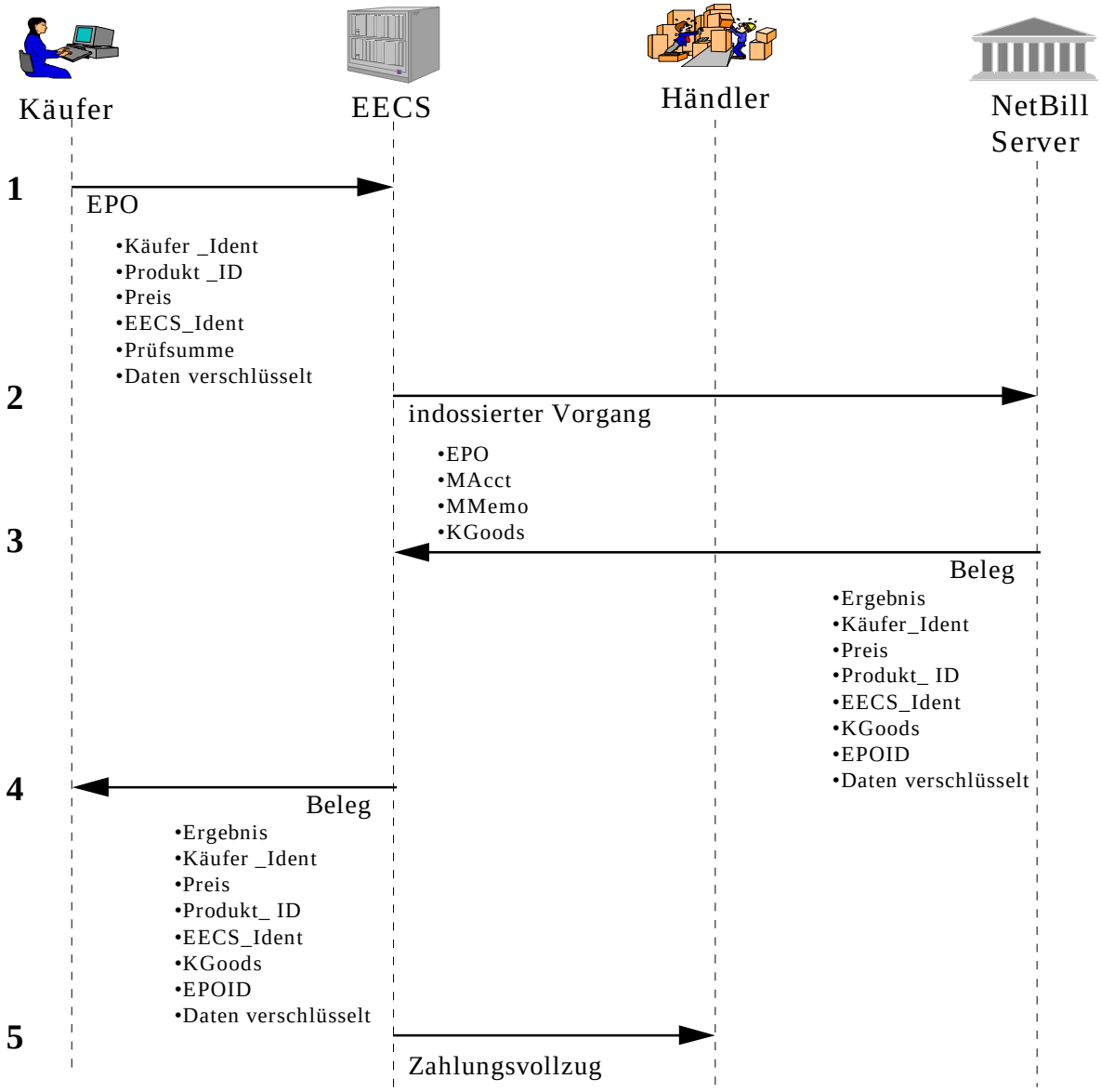


Abbildung 7-9; Geschäftsprozess NetBill - Zahlungsphase

1. Der Käufer initiiert die Zahlungsphase, indem er eine unterschriebene ***EPO***, die sich aus zwei Teilen zusammensetzt, an EECS versendet. Der eine Teil der *EPO* beinhaltet Details über die Transaktion (Käufer Identität, Produkt ID und

Preisspezifizierungen, EECS Identität, Prüfsumme der verschlüsselten Waren) und kann von EECS und NetBill Server gelesen werden, während der andere Teil Zahlungsinstruktionen (Ticket des Käufers, Käufer Kontonummer, Käufer Memo-Feld) enthält, die nur vom NetBill Server gelesen werden dürfen.

$T_{CM}, K_{CM}[EPO, Sig_C]$

2. EECS verifiziert die Unterschrift des Käufers, prüft, ob die Produkt_ID, der Preis und die Prüfsumme der Waren in Ordnung sind und leitet den zuvor **indossierten Vorgang** an den NetBill Server weiter. Zur Indossierung wird die EECS-Kontonummer (*Macct*), ein Memo-Feld (*MMemo*) und der Schlüssel K_{Goods} benötigt. Die gesamte Nachricht wird von EECS mit Sig_M unterschrieben an den NetBill-Server geschickt.

   $T_{MN}, K_{MN}[(EPO, Sig_C), MAcct, MMemo, K_{Goods}, Sig_M]$

3. Der NetBill Server entschlüsselt die Nachricht, belastet das Käuferkonto und erstellt einen ***Beleg***

   $Beleg = [Ergebnis, Käufer\_Ident, Preis, Produkt\_ID, EECS\_Ident, K_{Goods}, EPOID]Sig_N$

   Der NetBill Server ergänzt noch einige Konto-Statusinformationen und schickt folgendes an EECS:

   $K_{MN}[Beleg], K_{CN}[EPOID, CAcct, Kontostand, Flags]$

4. EECS entschlüsselt die Nachricht, behält eine Kopie und leitet den wieder mit K_{CM} verschlüsselten **Beleg** an den Käufer weiter.

   $K_{CM}[Beleg], K_{CN}[EPOID, CAcct, Kontostand, Flags]$

   Die Zahlung wurde ausgeführt und der Käufer kann den im Beleg enthaltenen Schlüssel K_{Goods} auslesen, um seine Informationsgüter zu entschlüsseln.

5. EECS schickt dem Händler eine Nachricht über den **Zahlungsvollzug**.

7.4.6 Geschäftsprozess Millicent

EECS übernimmt im Business-Modell von Millicent den Part des Brokers. Der Broker hat bei Millicent eine Aggregatfunktion, da er Micropayments eines Kunden bei verschiedensten Händlern ermöglicht, indem er Händler-Scrips (vgl. Kap. 6.2.4.1) ausgibt und gegen eine zuvor erfolgte Macropayment-Zahlung z. B. via SET verrechnet.

Die Verwaltung der Konten von Käufer und Händler obliegt dem Broker, der die Scrips der Händler an die Käufer weiterveräußert. Zwischen Broker und Händler besteht ein Vertragsverhältnis, das unter anderem festlegt, ob die Händler-Scrips vom Broker generiert werden, was wesentlich effizienter ist gegenüber dem Verfahren, daß der Broker die einzelnen Scrips Stück für Stück beim Händler kauft, bei sich zwischenspeichert und an die Kunden weiterverkauft.

Der Broker profitiert von seiner Vermittlertätigkeit über spezielle Preisnachlässe für Scrips, die auch den Aufwand für die Scrip-Generierung in Lizenz für den Händler abdecken und nicht an den Käufer weitergegeben werden.

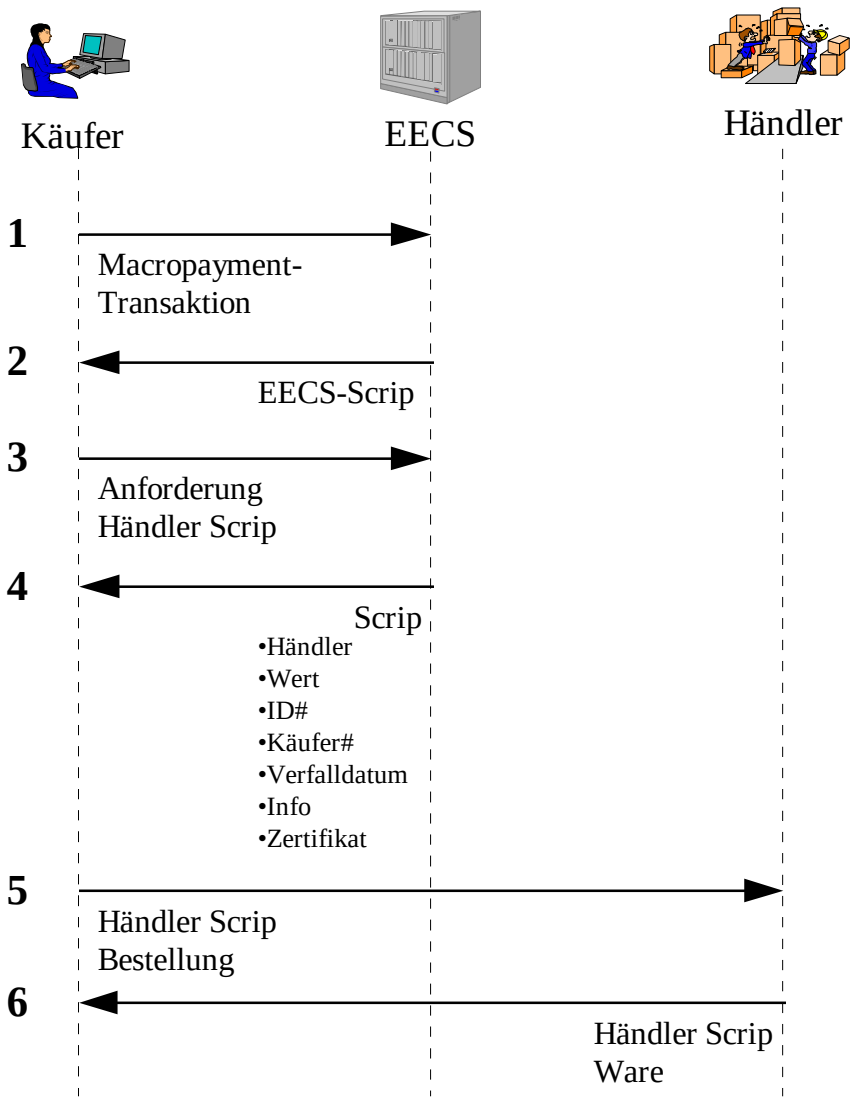


Abbildung 7-10; Geschäftsprozess Millicent

Der Ablauf einer Millicent-Transaktion [O'Mah97]:

1. Der Kunde deponiert einen Betrag auf seinem Millicent-Konto bei EECS über eine **Makropayment-Transaktion**
2. Über das Millicent-Protokoll erhält der Kunde **EECS-Scrip**.
3. Hat sich der Kunde zum Kauf bei einem Händler entschlossen, fordert er das spezifischen **Händler-Scrip** an.
4. EECS schickt das **Scrip** mit dem Aufbau:

   Scrip = {Händler, Wert, ID#, Käufer#, Verfalldatum, Info, Zertifikat}

   Die Feldbelegung:

   Händler enthält den Namen des Händlers, bei dem das Scrip Gültigkeit hat;

   Wert repräsentiert den Wert bzw. Restwert des Scrip;

ID#	ist eine eindeutige Nummer, die das Scrip identifiziert und die Möglichkeit des Double Spending einschränkt;
Käufer#	ist ebenfalls eine eindeutige Identifikationsnummer, die zur Berechnung eines Schlüssels herangezogen wird;
Verfalldatum	gibt an bis wann das Scrip gültig ist;
Info	ist ein frei belegbares Feld, dessen Inhalt von Händler und Broker festgelegt wird. Es enthält z. B. Käuferinformationen zur Entscheidung über Preiskonditionen, Rabatte, Boni, etc.;
Zertifikat	dieses Feld schützt das Scrip vor unbefugter Manipulation, mittels einer Hash-Funktion wird ein Wert generiert und abgespeichert, der als eine Art Unterschrift fungiert (digitale Signatur).

5. Der Kunde schickt das Händler-Scrip und die **Bestellung** an den Händler, der das Scrip auf Gültigkeit prüft.
6. Im Gegenzug erhält der Kunde die **Ware** und das im Wert angepaßte Händler-Scrip zurück.

Das Millicent-Protokoll sieht eine 3-stufige Sicherheitserweiterung vor, die je nach Anforderungen implementiert werden können. Die erste Stufe stellt die Übermittlung des Scrip im Klartext, wie oben beschrieben, dar. Die zweite Stufe ist um die Verschlüsselung mit einem gemeinsamen symmetrischen Schlüssel von Käufer und Händler erweitert. Für die dritte Stufe werden Signaturen für alle drei beteiligten Parteien (Händler, Käufer und Broker) eingeführt. Dies stellt die höchste Sicherheitsstufe dar, da durch diese Maßnahme Integrität, Authentizität und Vertraulichkeit gewährt sind, sowie das Problem des Double Spending lokalisiert werden kann.

7.5 Zahlungsströme

Um die Positionierung der Leistung von EECS deutlich zu veranschaulichen werden nun die Zahlungsströme zwischen den beteiligten Parteien beschrieben. Dies erfolgt getrennt nach Geschäftsprozessen, und berücksichtigt so die unterschiedlichen Verfahrensabläufe.

Ein grundsätzliches Unterscheidungsmerkmal der Ströme ist der **Auslöser**, der diese initiiert. Wir unterscheiden Zahlungsströme, die **bei jeder Transaktion** ablaufen, und Zahlungsströme, die durch die Abrechnung zu einem Stichtag, dem **Ultimo**, angestoßen werden.

7.5.1 Zahlungsströme bei Kreditkartenzahlungen

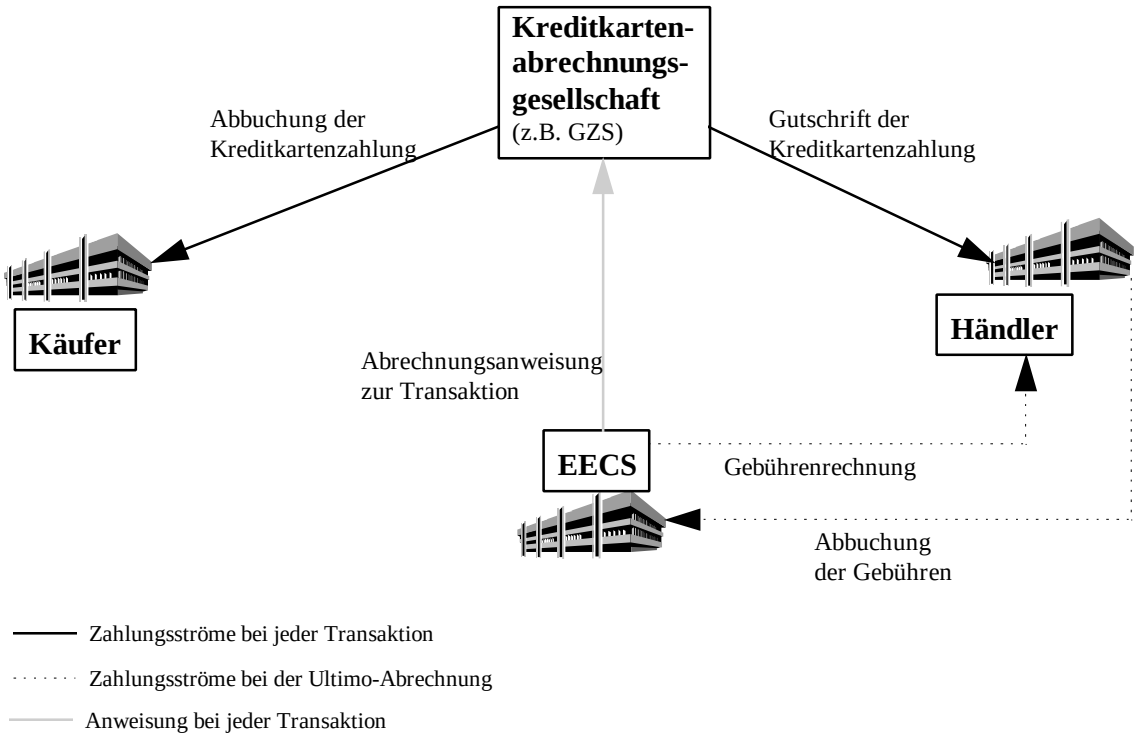


Abbildung 7-11; Zahlungsströme bei der Kreditkartenzahlung

Bei der Kreditkartenzahlung gibt EECS die Abrechnungsdaten der Transaktion an die Kreditkartenabrechnungsgesellschaft weiter, die das Clearing der Zahlung übernimmt. Die Kreditkartenabrechnungsgesellschaft veranlaßt die Abbuchung auf dem Käuferkonto und die Gutschrift des Betrages auf dem Händlerkonto.

Zum Stichtag werden die Gebühren von EECS ermittelt und in Rechnung gestellt.

7.5.2 Zahlungsströme bei Ecash oder NetBill

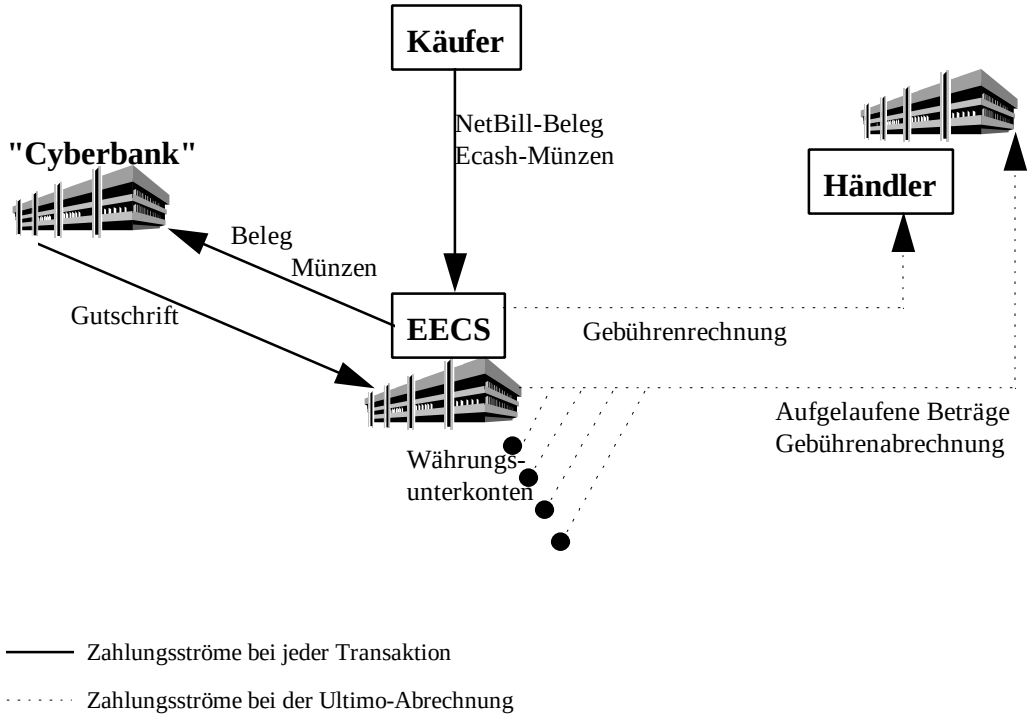


Abbildung 7-12; Zahlungsströme bei Ecash oder NetBill

Bei der Abrechnung von digitalen Münzen und elektronischen Schecks übernimmt EECS das Clearing mit der Ecash bzw. NetBill ausgebenden Bank, die in der obigen Abbildung als „Cyberbank“ bezeichnet wird. EECS wird bei den verschiedensten „Cyberbanken“ Konten unterhalten. Die von Käufern erhaltenen Münzen und Belege werden über diese Konten mit den Cyberbanken verrechnet.

Zum Stichtag führt EECS die Währungsumrechnungen durch und zieht die Währungsunterkonten zusammen, so daß dem Händlerkonto die aufgelaufenen Beträge in Deutsche Mark oder in einer anderen gewünschten Währung gutgeschrieben werden können. Der Gutschriftsbetrag ist um die von EECS einbehaltenen Gebühren reduziert.

7.5.3 Zahlungsströme bei Millicent

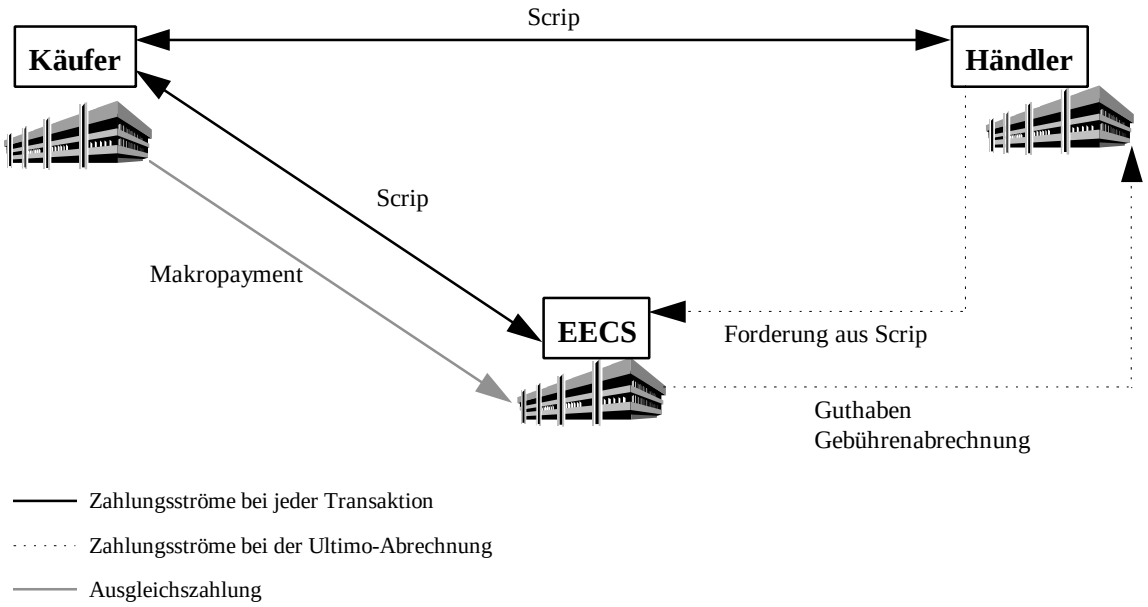


Abbildung 7-13; Zahlungsströme bei Millicent

Aus der im Business-Modell von Millicent definierten Rolle des Brokers, ergibt sich für EECS die Aufgabe, dem Käufer Scrips zur Verfügung zu stellen, als Gegenleistung für ein über ein Makropayment, z.B. Kreditkartenzahlung, deponiertes Guthaben.

Bei jeder Transaktion werden die Scrips ausgetauscht. Der Käufer tauscht EECS-Scrips gegen spezifische Händler-Scrips und bezahlt mit diesen beim Händler.

Zur Ultimoabrechnung werden die Händlerforderungen aus den gesammelten Scrips kumuliert und dem Händlerkonto, abzüglich der Gebühren, gutgeschrieben.

7.6 Zusammenfassung

Der geplante Funktionsumfang von EECS sieht keine Warenkorbfunktionalität vor, lediglich eine **Schnittstelle** zu Warenwirtschaftssystemen. Es ist keine Einflußnahme auf vor- bzw. nachgelagerte E-Commerce-Funktionen möglich. Dies hat den Vorteil, daß der Händler Funktionalitäten individuell gestalten kann. Zugleich entsteht aber auch ein Integrations- bzw. Anpassungsaufwand, der vom Händler, und bei Einbindung als Querschnittsdienstleistung in eine Mall vom Mallbetreiber, erbracht werden muß. Da die vorgegebene Schnittstelle bisher noch nicht näher spezifiziert wurde, kann keine Aussage über die Höhe des Aufwands gemacht werden. Wir können davon ausgehen, daß eine einfache Einbindung der EECS-Funktionalität in bestehende Internet-Anwendungen akzeptanzrelevant für das EECS-System ist.

Der Händler kann sein „***time-to-market***“ erhöhen, wenn er die EECS-Lösung, direkt oder aber über den Service der Mall, in seinen Shop einbindet. Für die beschriebene Vorgehensweise entsteht sicherlich ein geringerer Zeitaufwand, als für eine individuelle Umsetzung der Zahlungsabwicklung in einem Online-Shop.

Neben dem Installationsaufwand muß aber auch der Abrechnungsaufwand je Transaktion betrachtet werden, der durch die Inanspruchnahme der Querschnittsdienstleistung in der Mall, bzw. des primären EECS-Service für den Händler, auf ein Minimum reduziert wird.

Wie hoch die Akzeptanz bei einer **Gebührenpolitik** ist, die nur den Verkäufer mit den Gebühren für den Transaktionsdienst belastet, da nur dieser Vertragspartner von EECS ist, muß noch untersucht werden. Der Händler kann zwar die Gebühren anteilig auf die Online-Verkäufe umlegen, hierzu bedarf es aber zunächst eines Modells, wie die Kosten verteilt werden und wie sich dann die Kosten-/Nutzenrelation entwickelt.

Betrachtet man die **Situation der Konkurrenten** von EECS, so lassen sich direkte Konkurrenten, wie ICOMS[30] mit „Merchant Trax“ oder Internet Mall Inc. mit „OrderEasy“[31] identifizieren. Diese Unternehmen bieten neben der Bestellungs- auch die Zahlungsabwicklung als Outsourcer an [Sul97]. Bisher ist dieses Angebot jedoch auf die USA begrenzt.

Lösungsanbieter, wie z. B. CyberCash, haben sich im Markt etabliert. Diese Anbieter von Anwendungs-Lösungen müßen nicht als direkte Konkurrenten eingestuft werden, da sie bisher ihr Produkt am Markt anders plazieren, vielmehr wäre eine Kooperation mit EECS denkbar. Es kann aber davon ausgegangen werden, daß diese Unternehmen in naher Zukunft konkurrierende Dienstleistungen anbieten werden.

Mitbewerber könnten auch aus dem bestehenden POS-System kommen, wie z.B. Telecash, die nach eigenen Angaben ca. 100.000 Terminals[32] installiert haben und

---

[30] http://www.icoms.com

[31] http://www.ordereasy.com

[32] http://www.telecash.de/3_produkte

diesem Kundenstamm ihren Service rund um das bargeldlose Bezahlen anbieten. Dieses Kundenpotential und die Erfahrungen als zugelassener Netzbetreiber sind als Vertrauensbonus zu werten, den EECS sich noch mühevoll aufbauen muß. Eine Komplettlösung für WWW-Shop-Software mit integriertem Bezahlsystem „*TeleCash Internet*“ wird von Intershop Communications[33], Brokat[34] und TeleCash[35] zusammen auf den Markt gebracht.

Die dargelegte Konkurrenzsituation weist darauf hin, daß EECS als Anbieter der Querschnittsdienstleistung „Zahlungsabwicklung“, für eine von Shopping-Systemen unabhängige Mall, eine **Marktnische** belegt. Die konsequente Nutzung und der Ausbau dieses *unique-selling-points* gilt es umzusetzen.

Eine Möglichkeit die Erfolgschancen von EECS zu steigern wäre, **strategische Allianzen** einzugehen. Große Banken oder Kreditkartenunternehmen könnten mit einbezogen werden, um die Akzeptanz und das Vertrauen, das diesen Institutionen entgegengebracht wird, auf EECS zu transferieren. Ohne Vertrauen wird es schwierig bzw. nicht möglich sein, die Käuferakzeptanz zu gewinnen. Wie das Vertrauen der Internetnutzer in EECS im Einzelnen aufgebaut werden kann, muß noch ausführlicher geklärt werden. Hier besteht noch Forschungsbedarf.

[33] http://www.intershop.de

[34] http://www.brokat.de

[35] http://www.telecash.de

8 Plattform für das EECS-System

8.1 Vorgehensweise

„...*Wenn wir etwas Lebendiges, wie z.B. ein rechnergestütztes System, zustande bringen wollen, können wir es nur gestalten. Erst müssen wir die Gestalt vor Augen haben, dann die Bedingungen herstellen, daß unsere Vision wirklich Gestalt annehmen kann*....“ [Sie92].

Das Modell der Plattform für das EECS-System wurde mit objektorientierten Modellierungsmethoden modelliert. Die Annahme, daß die EECS-Applikation mit wiederverwendbaren, plattformunabhängigen, z. B. auf der Java Komponenten-Architektur (JavaBeans) basierten Applets umgesetzt werden wird, war für diese Entscheidung ausschlaggebend. Zudem eignet sich der objektorientierte Ansatz besonders für ein Vorgehensmodell mit Prototypingzyklen und einer starken Betonung von Analyse und Entwurf, was für die Umsetzung der Kontainerfunktionalität innerhalb der EECS-Applikation besonders geeignet scheint.

Eine schnelle, zeitsparende Entwicklung und Anpassung der Prototypen, durch die Möglichkeit der verstärkten Nutzung von Bausteinbibliotheken mit flexiblen Mechanismen, stellt einen weiteren Vorteil des objektorientierten Ansatzes dar [Neu95]. Diese Bausteinbibliotheken sind teilweise kommerziell verfügbar, wodurch sich der Programmieraufwand erheblich reduzieren läßt.

8.2 Architekturkonzept

Die relevanten Architekturmerkmale und deren realisierbare Ausprägungen zu identifizieren, ist das Ziel bei der Planung von Systemarchitekturen. In den frühen Planungsphasen sind jedoch nur Hauptmerkmale von besonderer Relevanz. Für die Erarbeitung einer ersten Grundarchitektur, beschränkt sich die Autorin dieser Arbeit auf die Beschreibung in Form eines informalen Architekturdiagramms.

Der Trend bezüglich IT-Systeme geht wieder hin zur Zentralisierung und schlanken Clients. Die Anwendungslogik wandert vom „fetten PC“, der alles lokal verfügbar hält, zum *Application-Server*. Es wird eine Client-Server-Architektur angestrebt, bei der vom Browser aus über eine Webseite plattformunabhängig Java-Applets heruntergeladen werden. Diese Client-Server-Architektur kann auch mehrstufig ausgelegt sein.

Der Aufbau des Architekturkonzepts wird in Abbildung 8-1; Architekturmodell veranschaulicht. Das Architekturkonzept besteht im wesentlichen aus drei Layern, die miteinander über offene Schnittstellen verbunden sind.

Der ***Application-Layer*** umfaßt die Interfaces und anwendernahen Prozesse und überspannt, wie ein Dach, den darunterliegenden Unterbau.

Der Unterbau besteht aus dem Secure Web Transaction Server, der zusammen mit dem Betriebssystem den untersten ***Basic-Layer*** bildet und dem ***Kontainer-Layer***, der säulenartig die Verbindung zwischen Basic- und Application-Layer herstellt.

Im Kontainer-Layer lassen sich Module einfach ergänzen oder austauschen, da sie durch die Kontainerfunktionalität gekapselt und somit schnell zu adaptieren sind.

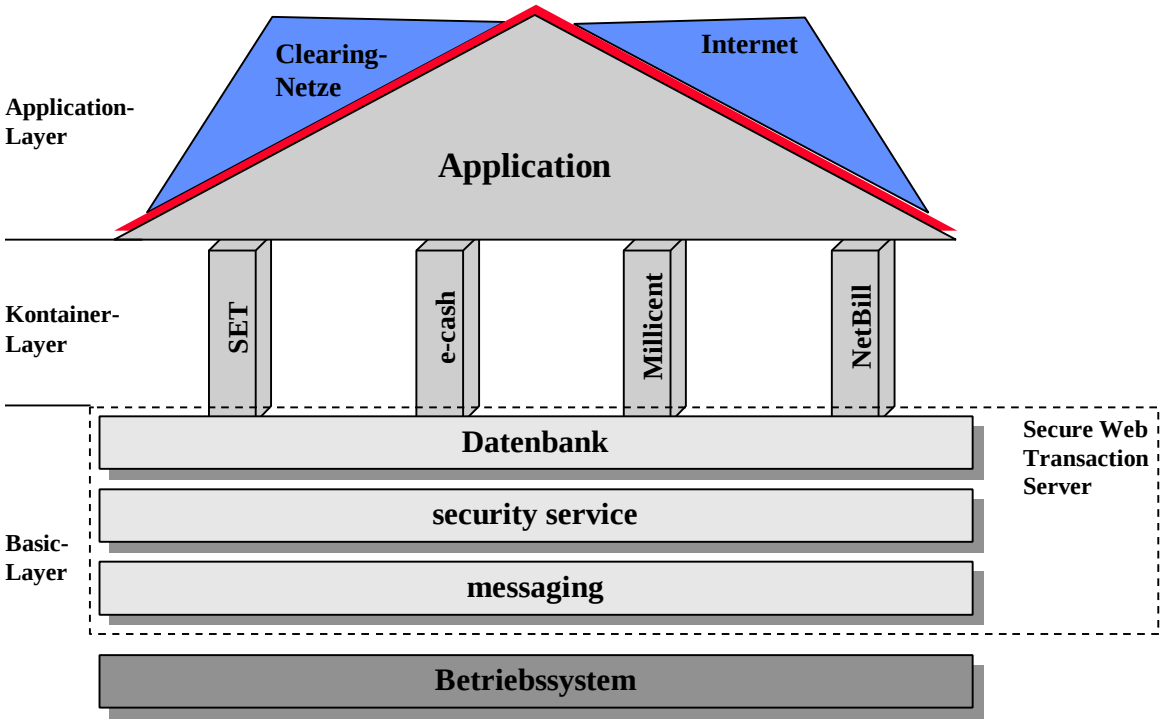


Abbildung 8-1; Architekturmodell

8.3 Datenkonzept

Die in der EECS-Transaktionseinheit anfallenden Daten können zunächst einmal grundsätzlich in die über öffentliche Netze, wie das Internet, zugänglichen Datenbestände und den Back-Office-Bereich unterteilt werden. Der durch Firewalls geschützte Back-Office-Bereich unterliegt höchsten Sicherheitsanforderungen, da hier hoch sensitive, äußerst schutzwürdige Daten gespeichert werden. Im Front-Office-Bereich, der geringeren Sicherheitsanforderungen genügen muß, werden die Protokolldaten gehalten. Der Zugriff auf die geschlossenen Clearing-Netzwerke der Banken und Kreditkartenabrechnungsgesellschaften über die Zahlungsmethoden-Kassetten wird hier verwaltet. Der Datenpool für die gesamte Internet-Kommunikation wird ebenfalls in diesem Bereich vorgehalten.

Die Organisationsstruktur der Datenbestände und deren wechselseitige Beziehungen werden in der Abbildung 8-2 dargestellt.

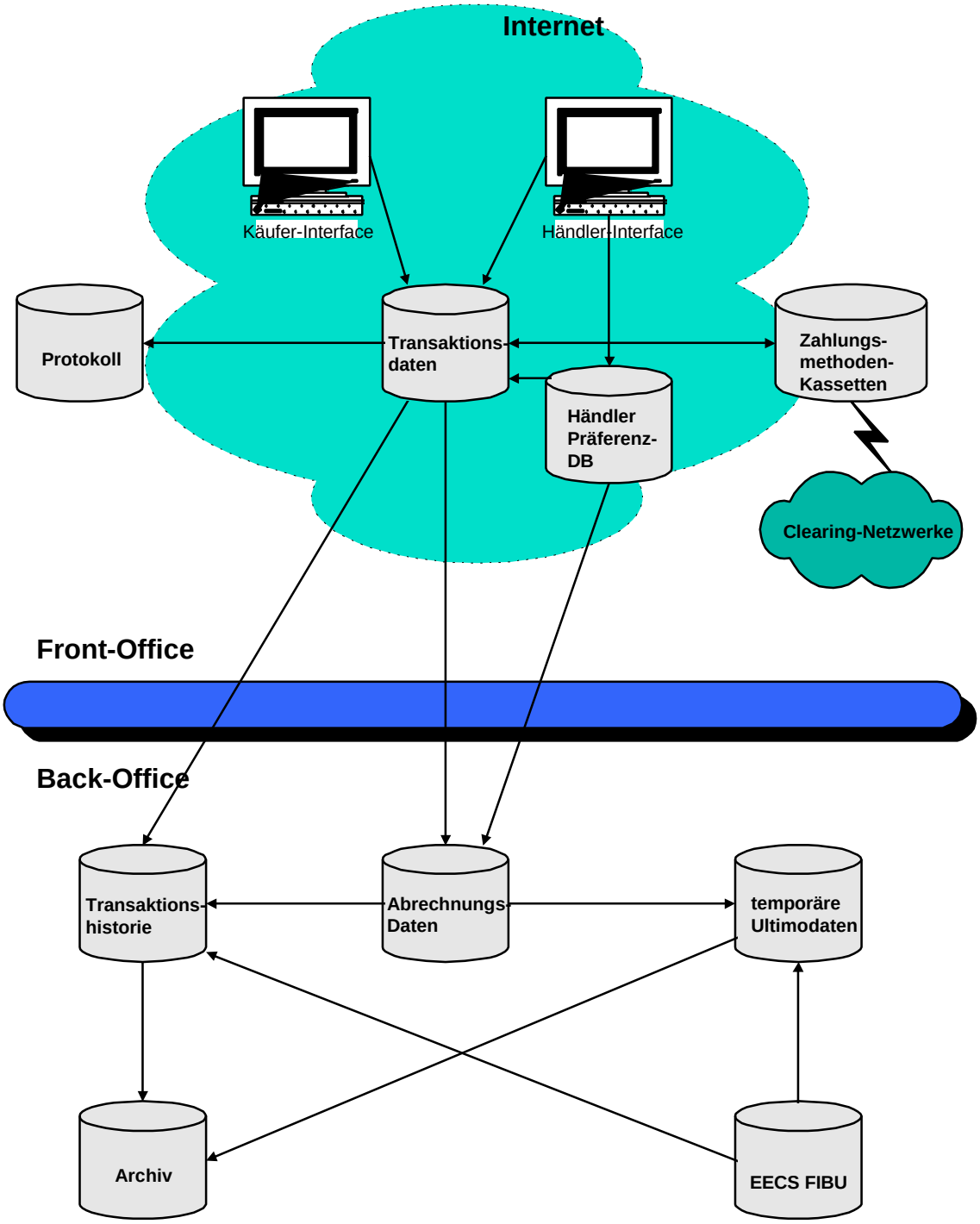


Abbildung 8-2; Organisation der Datenbestände

8.4 Grobdatenmodell

Es gibt verschiedenste Vorgehensweisen zur **Identifikation der Objekte**, die ein System bestimmen. Diese Vorgehensweisen sind nicht exklusiv zu sehen. Ein Designer kann sowohl Elemente aus der grammatikalischen oder szenariobasierten Analyse, als auch die Verwendung „greifbarer Entitäten“, Interaktionen, Ereignisse oder das Verhalten der Systempartizipanden zur Objektidentifikation heranziehen [Som95].

Bei der Identifikation der Objekte wurde in dieser Arbeit die Bottom-Up-Methode angewandt [Balz95]. Ausgehend von den gesammelten **Daten** (Attribute) aus den Interaktionsdiagrammen der Geschäftsprozesse (vgl. Kap. 7.4) und den **Funktionalitäten** (vgl. Kap. 7.3) konnten Klassen identifiziert werden.

8.4.1 Kunden

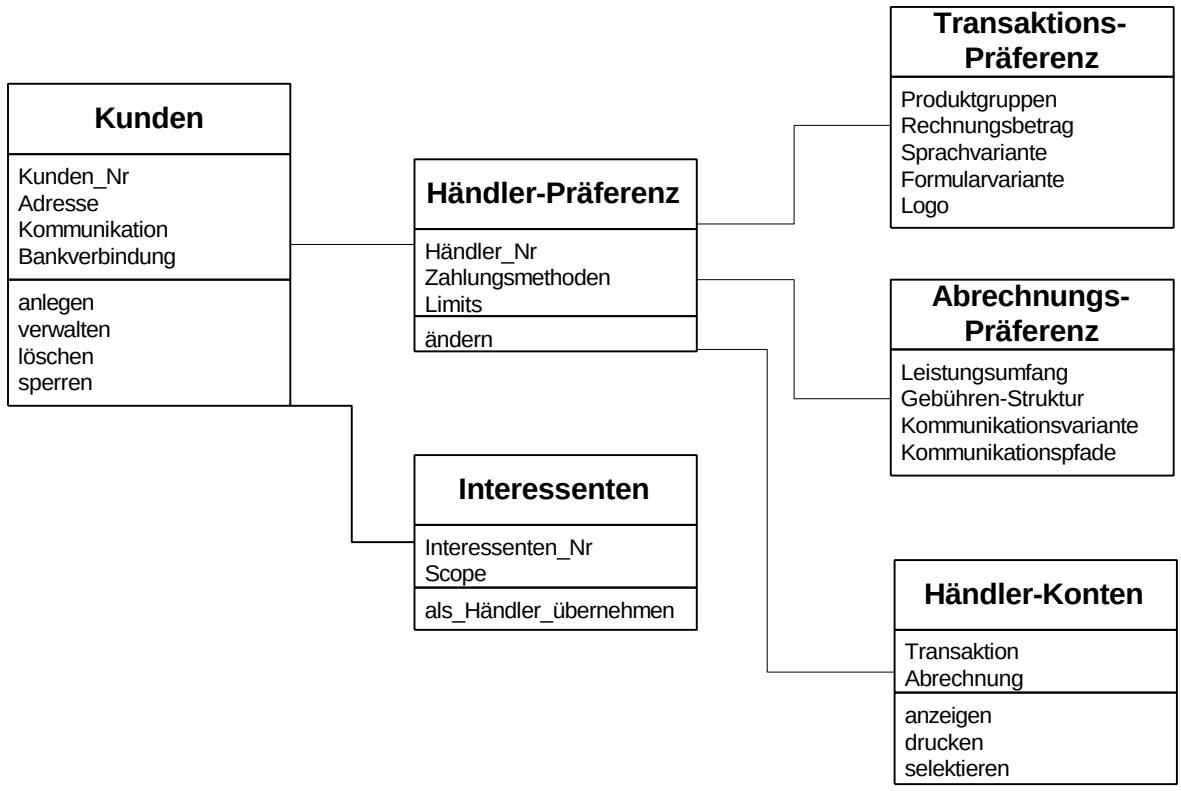


Abbildung 8-3; Klassendiagramm "Kunden"

8.4.2 Transaktion

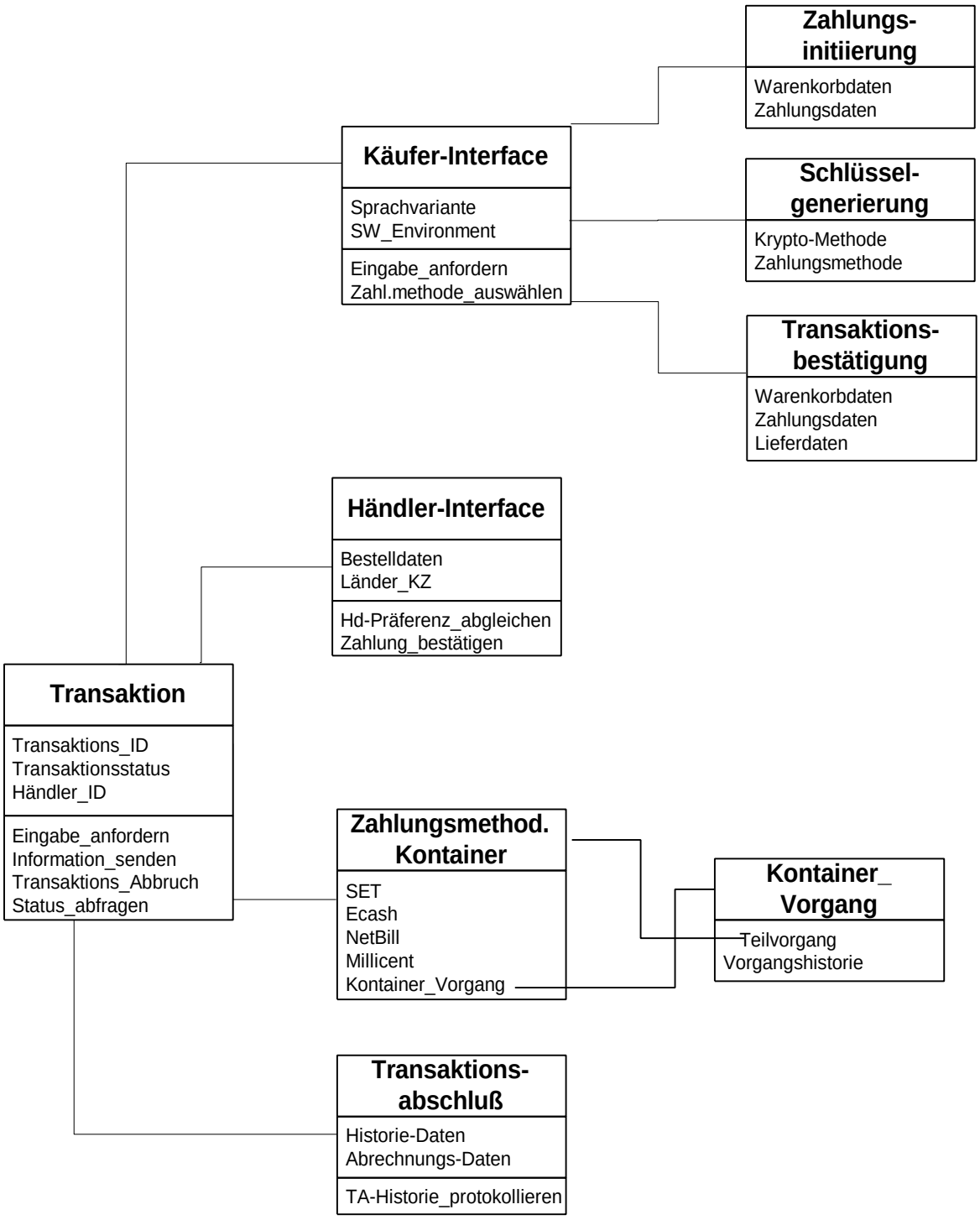


Abbildung 8-4; Klassendiagramm „Transaktion“

8.4.3 Historie-Daten

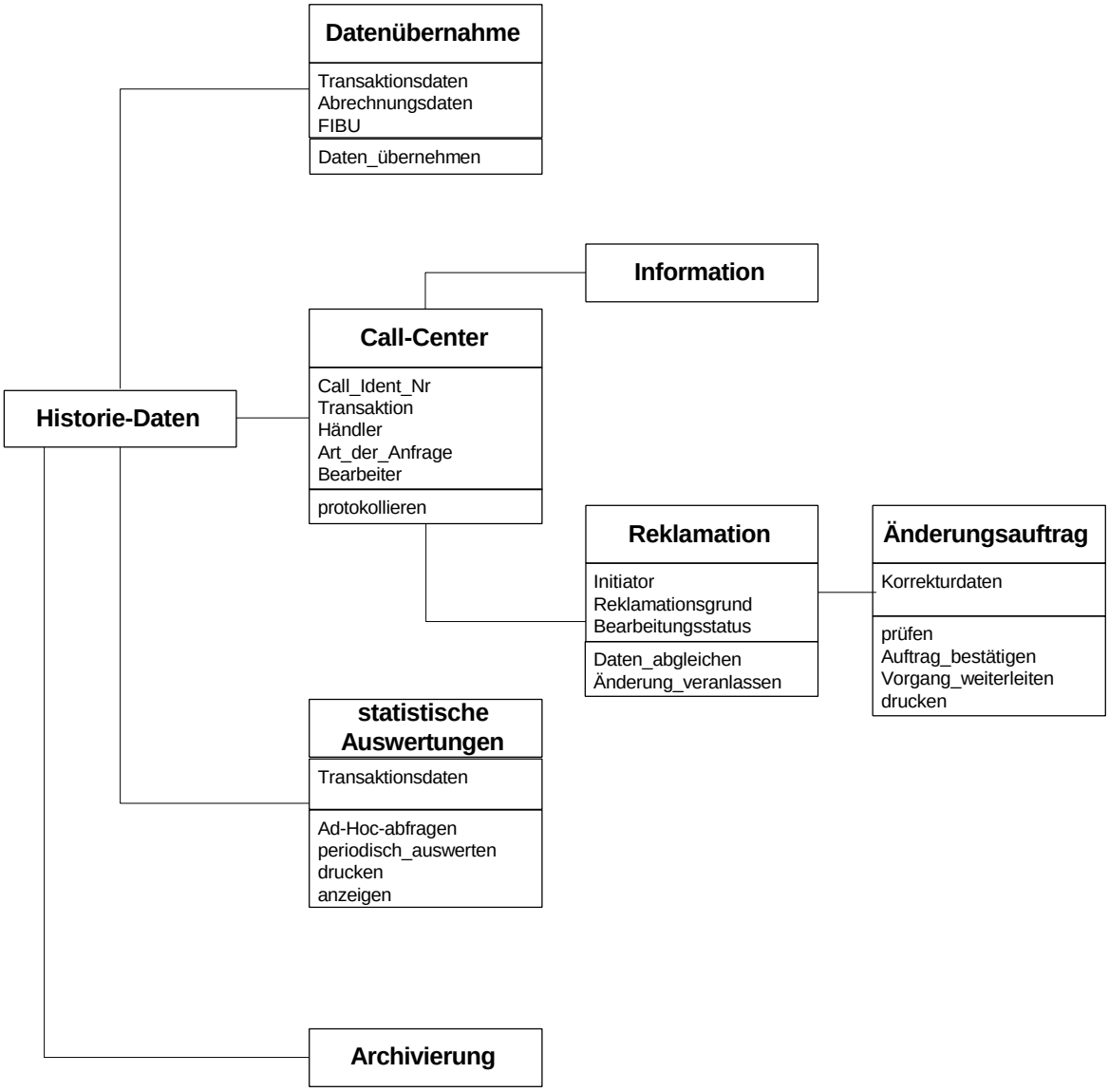


Abbildung 8-5; Klassendiagramm "Historie-Daten"

8.4.4 Abrechnungs-Daten zur Ultimoabrechnung

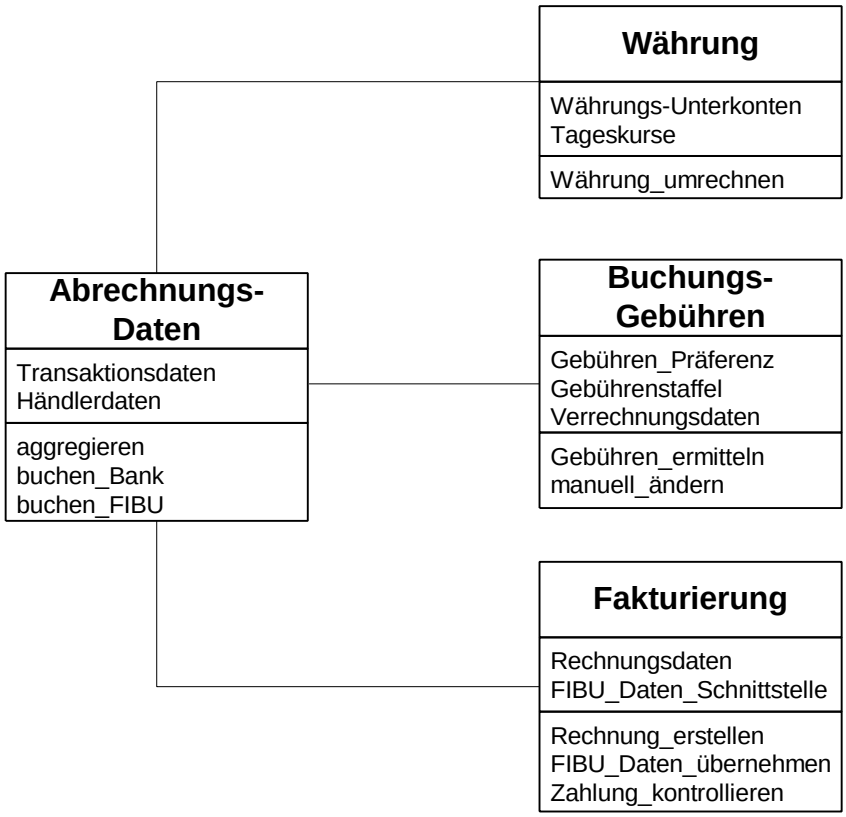


Abbildung 8-6; Klassendiagramm "Abrechnungs-Daten"

8.4.5 Netzverwaltung

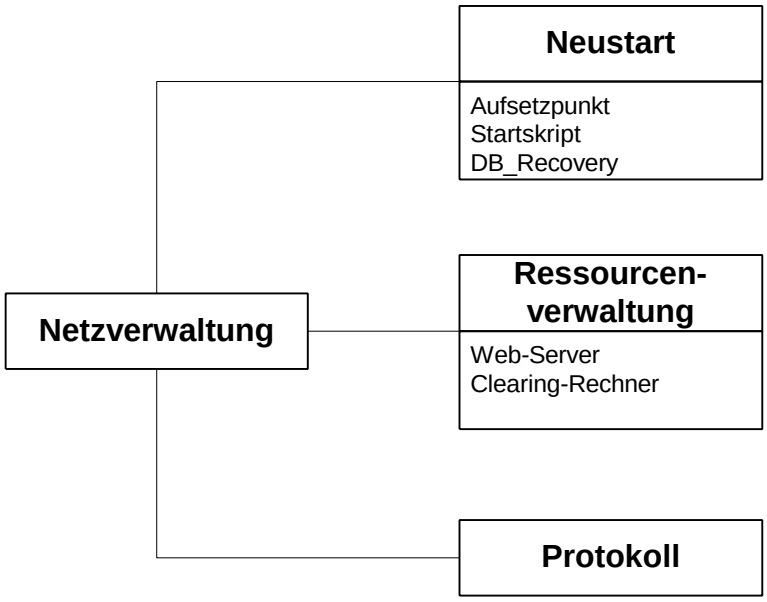


Abbildung 8-7; Klassendiagramm "Netzverwaltung"

8.5 Zusammenfassung

Das vorangestellte Kapitel vermittelt einen Überblick, aus drei verschiedenen **Perspektiven**, über das EECS-Gesamtsystem. Das Architekturkonzept beschreibt die Systemarchitektur, das Datenkonzept zeigt die Umsetzung der Systemanforderungen auf Datenebene und das Grobdatenmodell identifiziert Klassen des Systems. Das so spezifizierte System liefert die Grundlage zur softwaretechnischen Umsetzung des Modells.

8.5.1 Umsetzbarkeit des Modells

Durch die Verwendung von **Standards** und die Integration bestehender Software-Applikationen bzw. *Application Frameworks* wird versucht die Entwicklungszeit und damit auch das Projekt-Risiko zu minimieren. Die kurzfristige Fertigstellung ermöglicht ein schnelles „time-to-market", was als erfolgskritisch für das EECS-Gesamtsystem bewertet werden muß.

Durch die Verwendung von Java wird versucht das Ziel der **Plattformunabhängigkeit** zu erreichen. Die universelle Unterstützung ist zwar von der Theorie her definiert, aber in der Praxis können immer unvorhersehbare Probleme und Unwegsamkeiten auftreten. Wie sich die Standardisierungsbestrebungen und die Plattformunabhängigkeit für *Java* entwickeln ist fraglich, nachdem *Microsoft* offensichtlich aus dem *Java*-Standard ausschert.

Die Realisierung des EECS-Systems könnte mittels Developer Frameworks, wie z. B. *NCF (network computing Framework)* von *IBM*, das *Java* und *JavaBeans* einsetzt und im Leistungsumfang Gateways zu einer Vielzahl von standardisierten Software-Produkten zur Verfügung stellt erfolgen. Objektorientierte Frameworks für den Internet-Commerce, wie z.B. *CommercePoint* von *IBM*, *JECF* (*Java Electronic Commerce Framework*) von *Sun* / *Javasoft* oder *Microsoft Internet Commerce Framework*, um nur einige zu nennen, könnten genutzt werden. Welche hier zum Einsatz kommen sollten, wurde im Rahmen dieser Arbeit nicht untersucht. Eine Evaluierung der relevanten Systeme steht noch aus.

Klärungsbedarf besteht auch für die Frage, inwieweit branchenspezifische Software-Plattformen, wie z.B. die Integrations-Plattform „*Twister*" in Verbindung mit „*Pay-Line*", der Online Payment Infrastruktur, der Firma *Brokat*[36] einsetzbar sind. Hierbei sind nicht nur technische sondern auch unternehmens- und preispolitische Aspekte zu berücksichtigen.

8.5.2 Bewertung

Für die Beantwortung, der im vorigen Abschnitt aufgeworfenen Fragen, wird die in diesem Kapitel beschriebene Software-Plattform für EECS als **Grundlage** dienen. Zudem können die formalen Spezifikationen dazu beitragen ein **besseres Verständniss** für die Funktionsweise und den Umfang des EECS-Projekts zu vermitteln.

[36] http://www.brokat.de

Das in dieser Arbeit entworfene Modell erhebt keinen Anspruch auf Vollständigkeit, es spiegelt vielmehr den momentanen **Entwicklungs- und Kenntnisstand** des EECS-Projekts wieder. Die beschriebenen Strukturen und Klassen sind explizit erweiterbar konzipiert. Durch die modulare Kontainerfunktionalität, die es ermöglicht verschiedenste Module schnell auszutauschen oder zu ändern, wird die Erweiterbarkeit sichergestellt.

Auf einige Bereiche, wie beispielsweise die Warenkorbschnittstelle, die noch nicht ausreichend beschrieben und spezifiziert sind, wurde im Verlauf dieser Arbeit schon hingewiesen.

Wie die Einbindung der EECS-Dienstleistung als **Querschnittsdienstleistung** innerhalb einer Mall konkret zu realisieren ist, muß noch definiert werden. Es bietet sich an, die Schnittstellenspezifikation zwischen EECS und der Mall, als gemeinsames Projekt aufzusetzen, zumal die Querschnittsdienstleistungen bisher nur als semiformales Konzept existieren und seitens einer Mall noch keine dedizierten Beschreibungen vorliegen. Die zu erwartenden Interdependenzen zwischen dem Sammelwarenkorb der Mall (Querschnittsdienstleistung Warenkorb) und dem EECS-System könnten mittels dieser Vorgehensweise effizient umgesetzt werden.

Betrachtet man diese Interdependenzen, so stellt sich die Frage, ob die im EECS-Projekt propagierte Trennung des Warenkorbs und der Zahlungsabwicklung wirklich sinnvoll ist? Kann eine Schnittstelle geschaffen werden, die gesamtheitliche E-Commerce Transaktionen effizient abdeckt?

Die Einbindung des EECS Projekts in ein bestehendes, standardisiertes E-Commerce Framework, wie z. B. SEMPER oder OTP, in ihrem ganzheitlichen Ansatz, stellt eine gangbare Alternative dar. In diesem Umfeld wäre zum einen die Möglichkeit Kooperationen und Allianzen mit anderen Unternehmen einzugehen erleichtert, zum anderen könnte die bereits diskutierte Problematik des Vertrauensbonus, mit den richtigen Partnern, entschärft werden.

9 Ausblick

Das Kapitel Ausblick gliedert sich in Fazit und Schlußbetrachtung. Im Rahmen der Schlußbetrachtung soll der Gesamtkontext, in dem diese Arbeit steht, verdeutlicht werden und auch auf soziale und humanitäre Aspekte von allgemeiner Gültigkeit verwiesen werden. Während im Abschnitt Fazit auf die speziellen Entwicklungen eingegangen wird.

9.1 Schlußbetrachtung

Der Online-Handel wird einige **Wert- und Vertriebswege** zusammenbrechen lassen [Lyn97]. Geschäftsmodelle und die Rolle bzw. die Arbeit der Menschen kann sich dadurch drastisch ändern. Der Zwischenhändler könnte ausgeschaltet werden, da die Möglichkeit besteht direkt online beim Hersteller zu bestellen, auch wenn dieser beispielsweise in einem Land der Dritten Welt produziert und über herkömmliche Vertriebskanäle bisher nicht unmittelbar erreichbar ist. Im Einzelhandel könnte das Aufgabenspektrum auf die Funktionen Produktpräsentation und Kundenzentrum reduziert werden, da der Hersteller direkt an den Endkunden versendet und die Notwendigkeit einer Lagerhaltung wegfällt.

Eine Verlagerung der Wertschöpfung ist auch im Bereich **elektronische Heimarbeit** zu erwarten, wobei hier konträr zu der oben beschriebenen Reduktion eine Belebung abzusehen ist. Vor allem die Möglichkeit mit digitalem Geld Mikrotransaktionen vorzunehmen und Versand und Abrechnung online abzuwickeln, wird Auswirkungen auf die Effizienz der Heimindustrie haben. Ein besonderes Augenmerk ist hierbei auf „*weiche Produkte*“, die niedrige oder gar keine Herstellungskosten haben und durch zusätzliche Leistungen für eine *Veredelung* durch eine bestimmte Leistung prädestiniert sind, zu richten, wie z.B. Suchen, Sortieren, Indexieren, etc.

Unter dem Aspekt der einschneidenden Veränderungen in die Rolle des Menschen tauchen eine Vielzahl **sozialer und humanitärer Fragen** auf, die zum jetzigen Zeitpunkt noch nicht hinreichend geklärt sind.

Die neue Ära des Internet-Handels bietet uns die Möglichkeit die Logistik des Alltagslebens zeitsparender abzuwicklen und eine facettenreichere Kommunikation zu fördern. Es liegt bei jedem Einzelnen, mit welcher moralischen Verantwortung, die über Gerechtigkeit und Fürsorge definiert werden sollte [Gil36], er die gebotenen Vorteile nutzt und wie er auf die Gemeinschaft einwirkt, damit nicht zugelassen wird, daß die positiven Aspekte der neuen Entwicklungen pervertiert werden.

Alternativ könnten die aufgezeigten Möglichkeiten auch zur vollständigen *Versklavung* der Menschheit durch die absolute Kontrolle eingesetzt werden. Wir sind gefordert Sinn und Richtung zu wählen [Gor94], im Bewußtsein, daß sowohl Entscheidungen mit scheinbar geringer Tragweite, als auch solche mit offenkundig großen Auswirkungen, Einfluß auf den Entwicklungsverlauf nehmen.

Die Aussage, die Computertechnologie habe das Informationszeitalter hervorgebracht, ist irreführend. Die Computertechnologie ist nur ein weiterer Schritt von der Technokratie zum Technopol [Post91]. Der Grundstein für das Informationszeitalter wurde wohl schon viel früher gelegt. Alle uns bekannten Techniken und Technologien ermöglichen die Informationsgesellschaft[37], gleich der Steine in einem Mosaik, nicht nur die Computertechnologie.

Die Verschmelzung der Technologien miteinander und die Verbindung mit neuen Innovationen eröffnet Potentiale zur Realisierung von Synergieeffekten. Auf diesem Nährboden könnte für den **Electronic Commerce** bereits in naher Zukunft vermehrt die Forderung nach noch mehr Flexibilität und Mobilität [Schu97], gekoppelt mit einem Mehr an Sicherheit entstehen. Die Messlatte wird immer höher gesteckt. Es ist zu erwarten, daß unter Sicherheitsaspekten die Entwicklung hin zu hardwarebasierten Konzepten geht, wie z.B. Chipkarten, die als Multifunktionskarten, unter anderem auch als Online-Identitätsträger, ähnlich einem digitalen Personalausweis, eingesetzt werden können.

9.2 Fazit

Die zu erwartenden zukünftigen Entwicklungen, sowie identifizierbare Trends und Problemfelder für elektronische Zahlungssysteme werden nachfolgend umrissen. Diesem Abriss schließt sich eine kritische Betrachtung der in dieser Arbeit aufgezeigten Einsatz- und Entwicklungsmöglichkeiten von EECS an.

9.2.1 Elektronische Zahlungssysteme

Zu Beginn der gemeinsamen europäischen Währung am 1. Januar 1999 werden noch keine Barzahlungsmittel zur Verfügung stehen, der **EURO** wird nur als Buchwährung existieren. Dieser Umstand wird den elektronischen Zahlungssystemen einen deutlichen Aufwärtstrend geben [Mei96], da der *elektronische Euro* die Dringlichkeit der Bereitstellung von Münzen und Scheinen, im benötigten Umfang, abschwächen wird.

Diese positive Wirkung des Einsatzes neuer Zahlungssysteme geht aber auch einher mit **Gefahren für das Geldsystem**. Sowohl auf die nationale Währung als auch auf die internationalen Geldbewegungen sind Auswirkungen zu erwarten, die die monetäre Stabilität beeinträchtigen könnten [FuWr97]. Der Wirkungsgrad der Steuerungsinstrumente zur Geldwertstabilisierung über die Bargeldreserve, die von den Zentralbanken eingesetzt werden, könnte drastisch abnehmen. Dies ist kein grundsätzlich neuer Effekt. Durch den Rückgang des Bargeldanteils am Gesamtvolumen aller Geldformen, zu Gunsten der Kreditkartentransaktionen, ist dieser Effekt schon aus den vergangenen Jahren bekannt. Die Vermutung, daß die bereits bekannten Auswirkung auf die monetäre Stabilität durch die Innovationen verstärkt werden, liegt jedoch nahe.

---

[37] Definition nach Kuhlen: „Informationsgesellschaften sind dadurch gekennzeichnet, daß der Zugriff auf Wissensressourcen und die Fähigkeit, relevante Informationen aus ihnen zur Absicherung professionellen oder privaten Handelns zu erarbeiten, für ein aktives Mitwirken in allen gesellschaftlichen Bereichen entscheidend sind.“ [Kuhl95a, S.48]

Die Einbeziehung elektronischer Zahlungssysteme in die staatliche Währungshoheit scheint auf lange Sicht erstrebenswert, da die Systeme auf das **Vertrauen der Marktteilnehmer** angewiesen sind. Sietmann geht davon aus, daß die Marktkräfte allein keine stabilen Strukturen schaffen werden, so daß eine frühzeitige Kooperation der Notenbanken, zur Schaffung geeigneter Rahmenbedingungen für die Rechts- und Geldwertsicherheit, auf supranationaler Ebene wünschenswert ist [Siet97].

Ein weiterer öffentlicher Aspekt liegt in der berechtigten Sorge, hinsichtlich der durch elektronische Zahlungssysteme eröffneten Möglichkeiten, der Steuerhinterziehung und Geldwäsche. Auch hierbei scheinen keine grundlegend neuen Effekte identifizierbar, vielmehr sind die medialen Einsatzmöglichkeiten neu und bedingen eine Umgestaltung von bestehenden Modellen und die **internationale Harmonisierung** der Kontroll- und Eingriffsmöglichkeiten. Wenn erst einmal die Frage der Abrechnung und Authentifizierung im Internet zufriedenstellend gelöst ist, steht einem virtuellen Outsourcing der steuerrelevanten Gewinne nichts mehr im Wege. Unternehmen könnten es leicht haben, ihre Gewinne dort anfallen zu lassen, wo die Steuersätze niedrig sind.

Eine Verquickung der Systeme unter **multifunktionalen** Aspekten, als auch das Verschmelzen bestehender Infrastrukturen, wie z.B. Telefon, Briefpost und Fernsehprogramme, in ein weltumspannendes Datennetz ist zu beobachten. Dieser Trend ist auch für Zahlungssysteme und Online-Banking-Anwendungen auszumachen. Kartengestützte Zahlungssysteme und Zahlungssysteme im Internet könnten verschmelzen. Für Deutschland ist zu erwarten, daß die bundesweit eingeführte GeldKarte zur Multifunktionskarte wird, die sowohl im Selbstbedienungsbereich der Banken, innerhalb der POS-Infrastruktur und vom heimischen PC aus zur Zahlungsabwicklung eingesetzt werden kann.

Internetbasierte Systeme zur Rechnungsabwicklung, wie z.B. Electronic Bill Presentment and Payment (EBPP[38]), integriert in *Personal Finance Management Software* werden dem Endbenutzer zur Verfügung stehen.

In Anbetracht dieser Entwicklungstendenzen, wird die Bedeutung des **Datenschutzes**, bzw. der Anonymität zum Schutz der individuellen Privatsphäre, und der hohe Stellenwert von **Vertrauen** deutlich. Es stellt sich die Frage, wie ein effektiver Datenschutz gewährleistet werden kann und welche Möglichkeiten es gibt Vertrauen zu etablieren?

Sietmann geht davon aus, daß **Sicherheitsbedenken**, bei aller gebotenen Vorsicht, kein wirkliches Hemmniss für den Erfolg elektronischer Zahlungssysteme darstellen [Siet97 S.159]. Diese Einschätzung steht konträr zu den Ergebnissen der „Electronic Commerce Enquete“, bei der 66 Prozent der Befragten die Unmöglichkeit sicherer Zahlungen über das WWW als größte Hürde einstuften. Welche Kriterien fließen in die Sicherheits- und Risikobewertung eines Systems durch die Partizipanden ein? Wie kann eine mehrseitige Sicherheit, wie in Kapitel 4.1.2 beschrieben, erreicht werden?

[38] http://www.msfdc.com

Es kann davon ausgegangen werden, daß der Erfolg elektronischer Zahlungssysteme eng mit der Beantwortung dieser offenen Fragen verzahnt ist.

Die aktuellen Zahlungssysteminnovationen für das Internet zeigen, daß meist versucht wird herkömliche, bewährte Konzepte für Zahlungsinstrumente zu adaptieren. Welche Zahlungssysteme im Einzelnen sich durchsetzen werden ist noch fraglich. Die Umsetzung des **SET-Standards** ist jedoch als wichtiger Erfolgsfaktor einzustufen. Unter internationalen Gesichtspunkten muß davon ausgegangen werden, daß HBCI mittel bis langfristig von SET verdrängt wird, oder aber HBCI in den SET-Standard integriert werden wird.

Bei den künftigen Neu- und Weiterentwicklungen der Zahlungssysteme, besteht die Herausforderung darin, ein mittleres Niveau zwischen Homogenisierung und Differenzierung zu finden [Rie98]. Das Zahlungssystem der Zukunft sollte offen genug für die Realisierung spezifischer Anforderungen und einheitlich genug für die breite Nutzungsakzeptanz sein. Auf Basisstandards aufsetzende, offene Systeme sind hierfür besonders geeignet.

Im Internet wird sich, genau wie im konventionellen Geldverkehr, ein **Verbund aus Systemen** etablieren, der die verschiedenen Kundensegmente abdeckt. Zahlungssystem-Service-Anbieter werden kooperieren, oder ein Dienstleister wird in Lizenz eine breite Palette von Systemen anbieten, um eine größere Segmentabdeckung zu erreichen.

9.2.2 EECS

Die ganzheitlichen Ansätze von **SEMPER** und **OTP** können wir als zukunftsweisend einstufen. In Zusammenarbeit mit solchen internationalen Forschungs- und Entwicklungsprojekten hätte EECS gute Chancen, das Potential seiner Idee nutzenbringend umzusetzen. Das in dieser Arbeit angefertigte Modell einer Software-Plattform könnte als Grundlage für das Aufsetzen auf einem offenen Basisstandard herangezogen werden.

EECS hat keine aktuellen, verläßlichen Zahlen über die Akzeptanz von Online-Shoppern für einen zusätzlichen Finanzintermediär vorliegen. Die im Geschäftsplan verwendeten Wachstumsprognosen entstammen der Internet-Suchmaschine „Yahoo“ [EECS97] und können schwerlich als fundiert eingestuft werden. Um jedoch die Erfolgsaussichten realistisch einschätzen zu können bedarf es gesicherter Erkenntnisse über die Konsumentennachfrage. Eine **qualifizierte Marktstudie** sollte durchgeführt werden, da diese nicht nur wünschenswert, sondern eine Grundvoraussetzung für die differenzierte Beurteilung des Marktes darstellt.

Die Situation der **Gebührenordnung** ist ungeklärt. Was wird von den Händlern, respektive den Kunden toleriert? Zum jetzigen Zeitpunkt ist noch unklar, was der Markt akzeptiert.

Wir befinden uns wohl erst am Anfang einer Lernkurve, wie das Gesamtsystem Internet, inclusive seiner Teilnehmer, interagiert. Die Frage der Gebührenakzeptanz steht eng im

Zusammenhang mit den zur Zeit heftig diskutierten Fragen nach dem **Preismodell** für die Internet-Nutzung selbst. Vorstellbar ist auch ein alternatives Finanzierungsmodell über Werbefinanzierung oder Abonnementmodelle.

Die Entwickler elektronischer Zahlungssysteme orientieren sich an den Handelserfordernissen, deshalb ist die zu beobachtende Ausbildung von untereinander inkompatiblen „Währungsinseln“ keine Besonderheit, sondern ein natürlicher Wesenszug der Geldentwicklung [Siet97]. EECS könnte diesen Umstand nutzen um als intermediärer ***Online-Geldwechsler*** im Markt zu agieren. Dieser Service würde über bereits geplante in dieser Arbeit beschriebene Leistungsmerkmale der Währungskonsolidierung zum Ultimostichtag hinausgehen. Es stellt sich jedoch die Frage, ob EECS die Konvertibilität der ausgetauschten Werte in die nationalen Währungssysteme sicherstellen kann? Verlangt der Markt überhaupt nach einer solchen Dienstleistung? Wenn ja, wann?

Die Macht der Banken und der hohe Reglementierungsgrad, z.B. des deutschen Finanzdienstleistungssektors, stellt eine große Zugangsschwelle für EECS dar. Für ein finanzschwaches, noch unbekanntes Unternehmen, wie EECS, ist es nicht erfolgversprechend als **Konkurrent** zu den etablierten Finanzdienstleistern aufzutreten, vielmehr sollten Kooperationen mit diesen Unternehmen angestrebt werden. Es muß davon ausgegangen werden, daß nur wenn *„Große mit im Boot sitzen“* EECS eine Chance haben wird, sich im nationalen und internationalen Markt zu behaupten.

Im Markt werden kapitalstarke, einflußreiche Banken, Organisationen und etablierte Unternehmen, wie z.B. die Kreditkartenabrechnungsgesellschaft GZS, die auf Grund ihrer Marktstellung schon Vertrauen auf sich bündeln und das nötige Prozess-Know-How haben, ähnliche Finanzdienstleistungen anbieten. Diese Szenarien wurden bisher noch nicht ausreichend untersucht, ebenso wie die Evaluation potentieller Konkurrenten zum jetzigen Zeitpunkt. Diese grundlegenden Informationen aktuell zu beschaffen, muß der nächste Schritt in der Entwicklung von EECS sein.

Es bleibt anzumerken, daß ein **Patent**, besonders eines in der Software-Branche, keinen Schutz vor Mitbewerbern im Marktsegment bietet, es erleichtert lediglich den Start und die Risikokapitalbeschaffung. Während diese Arbeit entsteht, ist die Finanzierung der Geschäftsidee von EECS noch nicht gesichert. Interessenten aus der *Venture-Capital-Sparte* für das Projekt gibt es einige. Die Zuversicht in einen prosperierenden E-Commerce im Internet ist weit verbreitet. Ob eine Dienstleistung wie die der EECS kurz- bis mittelfristig nachgefragt wird, wird die Zukunft zeigen.

Anhang A

Patentschrift, unter der Anmeldung Nr. 97110207 .4-2207-

Bezeichnung:

Transaktionseinheit-/Transaktionsverfahren zur Zahlungsabwicklung im Internet und/oder ähnlichen öffentlichen Client-Server-Systemen

Die Unterlagen liegen beim Europäischen Patentamt vor.

Literaturverzeichnis

[Ara97] Aranda, A.: „Kundenbindungsstrategie mit Chipkarte“; http://www.winforms.phil.tu-bs.de/winforms/company/solaic/

[Balz95] Balzert, Heide: „Methoden der objektorientierten Systemanalyse“; Mannheim, Leipzig, Wien, Zürich: BI-Wiss.-Verlag; 1995

[Bar97] Bartmann, Dieter / Fotschki, Christiane: „Elektronische Geldbörse“; Gutachten der Friedrich Ebert Stiftung, Bonn, 1997

[Bir98] Birkelbach, Jörg: „Geldgeschäfte im Netz - Ernüchternd: Plakative Anwendung ohne Anwendernutzen“; in Die Welt vom 19.3.1998 http://www.welt.de

[Bön95] Böndel, B.: “In Fallen tappen“; in Wirtschaftswoche Nr. 42, Jg. 49, vom 12.10.1995: S. 126ff

[Budd96] Buddemeier, Heinz: „Was wird im CyberSpace aus den sozialen Beziehungen“; in *Cyber Space, Virtual Reality: Fortschritt und Gefahr einer innovativen Technologie*; hrsg. von F. Wedde; Stuttgart 1996

[Bull96] Bullinger, Hans-Jörg: „Virtual Reality - eine innovative Technologie an der Schwelle zum 3. Jahrtausend“; in *Cyber Space, Virtual Reality: Fortschritt und Gefahr einer innovativen Technologie*; hrsg. von F. Wedde; Stuttgart 1996

[Büll98] Prof. Dr. Bernd Büllesbach, Konzernbeauftragter für den Datenschutz Daimler Benz AG; BSI-Diskurs Bonn, 5.2.1998

[BusMed96] BusinessMedia/51 Bericht; von Himmelspach, A. / Runge, A. / Schubert, P. / Zimmerman, H.-D.: „Anforderungen an elektronische Zahlungssysteme“; Hochschule St. Gallen, Version 1.0, Oktober 1996

[c’t 16/97] Kossel, Axel / Wronski, Hans-Jürgen: „Bare Bytes, Online bezahlen im Internet“; in: c’t 1997, Heft 16, S. 66-69

[Cav95] Cavalli, Dr. Alexander: „Electronic Commerce and the Internet: Bulding a New Paradigm for Business“; White Paper, Strategic Development; Trade Wave Corporation; Mai 1995

[CODAT96] Commerzbank, „Datenträgeraustausch Kunde/Bank“; Herausgeber Bundesverband Deutscher Banken e. V.; Bank Verlag GmbH, Köln; 1996

[CW4/98] „Studie: E-Commerce-Umsätze erreichen 2001 in Europa 64,4 Milliarden Dollar“; o. V.; Highlights vom 7.4.1998 http://www.computerwoche.de

[Der96] Dery, Mark: „Cyber - Die Kultur der Zukunft“; Grove Press, New York 1996

[DrDu98] Dresen, S. / Dunne, Th.: „Fürs Netz geprägt - Wie CyberCash funktioniert“; in iX - Magazin für professionelle Informationstechnik, April 1998, S. 110-116

[Dys98] Dyson, Esther: „Wie das Internet das Zusammenleben verändern wird“; in Office Management 1/98; S. 64-65

[ECE97/98] „Electronic Commerce Enquete 97/98“; gemeinsame Studie des Instituts für Informatik und Gesellschaft / Abteilung Telematik der Universität Freiburg, Computer Zeitung und Gemini Consulting; Herbst 1997 http://www.iig.uni-freiburg.de/~schoder/ece

[ECIN98] Electronic Commerce Info: „Internetfähige elektronische Zahlungssysteme im Vergleich“; Stand Februar 1998 http://www.electronic-commerce.org

[EECS97] Grunert, Rainer / Hoffmann, Sigrid / Semar, Wolfgang / Waltemathe, Horst / Wolf, Annette : „Geschäftsplan der EECS, European Electronic Cash System“, Stand 28. Oktober 1997

[euro.de] Webseite des Europäischen Parlaments, „Wann kommt der Euro?“ http://www.europarl.de/euro/frage2.htm

[EwWa93] Ewald, J. / Waldocks, J : „Plastic Money Terminology. An English-German Glossary“; Bd. 109; 1993

[FuWr97] Furche, A. / Wrightson, G. : „Computer Money : Zahlungssysteme im Internet“; dpunkt-Verlag, Heidelberg 1997

[GePo98] Geist, Marc-Rene / Popp, Heribert: „Virtual Reality (VR) - Anwendungssysteme zur Verkaufsunterstützung“; in Wirtschaftsinformatik, Heft 1, 40. Jahrgang, 1998/1; S. 33-38

[Gil36] Gilligan, Carol: „Gerechtigkeit und Fürsorge“; in Lesebuch zur Ethik, Hrsg. O. Höffe; Beck’sche Reihe, München 1998; S. 401-405

[Gö/Se97] Görke, Klaus / Semar, Wolfgang: „Electronic Commerce: Konzepte, Standards und Entwicklung von interaktiven Transaktionsformen im Internet“; Informationswissenschaft Bericht 82-97, Universität Konstanz, April 1997

[Goeb97] Goebels, Udo: „Entwicklungskonzept für virtuelle Marktplätze am Beispiel der EMB“, Konstanz, 23.7.1997

[Gom98] Gomez-Saez, Carlos,: „EZI-L Lastschrift“, vom 7.4.1998 ezi-l@listserv.fzk.de

[Gor94] Gore, Al: „Wege zum Gleichgewicht - Ein Marschallplan für die Erde“; Fischer Taschenbuchverlag GmbH; Frankfurt, Juni 1994

[Grun97] Grunert, Rainer: „Interessenanalyse - Internet Zahlungsmittel“; Schwalbach, 1997

[HBCI97] Homebanking-Abkommen vom 1.10.1997

[HBCI98] „HBCI - Hombanking-Computer-Interface „ Schnittstellenspezifikation; herausgegeben von: Bundesverband deutscher Banken e.V., Köln, Deutscher Sparkassen- und Giroverband e.V., Bonn, Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Bonn, Bundesverband Öffentlicher Banken Deutschlands e.V., Bonn Version 2.0.1 vom 2.2.1998

[Her98] Herreiner, Dorothea K.: “Führen die neuen Zahlungssysteme zu volkswirtschaftlichen Turbulenzen?“; BSI-Diskurs Bonn, 5.2.1998

[Herz97] Herzberg, Amir / Yochai, Hilik: „MiniPay: charging per click on the Web“; in Computer Networks and ISDN Systems, Volume 29 (1997), S. 939 - 951

[Herz98] Herzberg, Amir: „Safeguarding Digital Library Contents - Charging for Online Content“; D-Lib Magazine, Januar 1998; http://www.dlib.org/january98/ibm;

[HerzS98] Herz, Stephen (senior vice president of electronic commerce at Visa International); zitiert in: „Ready, SET, Still Not Ready To Go“ von Connie Guglielmo; http://www.zdnet.com/intweek/daily; 23.03.1998

[Him96] Himmelspach, Andrea: „Analyse und Bewertung von elektronischen Zahlungssystemen“; Hochschule St. Gallen, Bericht zu BusinessMedia/52, Version 1.0, Oktober 1996

[HiZi96] Himmelspach, A. / Zimmermann, H.-D.: „Elektronische Zahlungssysteme als kritischer Erfolgsfaktor des Electronic Commerce in offenen Telematikstrukturen“; in Informatik Nr. 6, Dezember 1996, S. 18-25

[Höf96] Höflich, Joachim R.: “Technisch vermittelte interpersonale Kommunikation“; Westdeutscher Verlag Opladen, 1996

[Kam97] Kambil, Ajit: „Doing Business in the Wired World“; in Computer - Innovative technology for computer professionals, Mai 1997, Seite 56-61

[Kol98] Kollmann, Karl: „Verbraucher und Sicherheit bei elektronischen Transaktionen“; BSI-Diskurs Bonn, 5.2.1998

[Kuhl2/98] Kuhlen, Rainer: „Foren gehoeren zu eMarktplaetzen - EMB nicht nur virtuelles Verzeichnis“; in emb Forum, Verschiedenes, Beitrag vom 21.2.1998

[Kuhl95a] Kuhlen, Rainer: „Informationsmarkt: Chancen und Risiken der Kommerzialisierung von Wissen“; Konstanz: UVK, Univ.-Verl., 1995

[Kuhl95b] Kuhlen, Rainer: „Elektronische regionale Märkte als kooperative Netze“; in: *Informationsmanagement in der Informationsgesellschaft*, Proceedings des 2. KIK; 27./28. Oktober 1995

[Kuhl96] Kuhlen, Rainer: „Zur Virtualisierung von Regionen durch elektronische Marktplätze“, Bericht 79-67, Konstanz, September 1996

[KuTe97] Kurbel, K. / Teuteberg, S.: „Betriebliche Internetnutzung in der Bundesrepublik Deutschland. Ergebnisse einer empirischen Untersuchung“; Arbeitsbericht Dezember 1997 http:///viadrina.euv-frankfurt-o.de/~wi-www

[KWG97] „Kreditwesengesetz - mit weiteren Vorschriften zum Aufsichtsrecht der Banken“; 51. Ergänzungslieferung von Manfred Schneider; Beck’sche Verlagsbuchhandlung; München, Stand Oktober 1997

[Lac97] Lacoste, Gerard: „A Security Framework for the Global Electronic Marketplace“; SEMPER document 431LG042 vom 25. August 1997; http://www.semper.org

[Lan98] Lange, Barbara: „Mausklick-Preise ; Abrechnung von Kleinstbeträgen im Internet“; in iX - Magazin für professionelle Informationstechnik; 1 / 1998, S. 119 - 121

[LiRu97] Lindemann, Markus / Runge, Alexander: „Permanent IT-Support in Electronic Commerce Transactions“; in em - International Journal of Electronic Markets, Vol.7, Nr. 1, 1997, S.18 - 20

[Löh98] Löh, A.: „Intrusion Detection System“; Vortrag im Seminar *Sicherheit von Informationssystemen*, vom 6. Februar 1998 http://www.informatik.uni-konstanz.de/ dbis/Publikations.htm

[Luk97] Lukas, Sylvia: „Cyber Money - Künstliches Geld im Internet und Elektronische Geldbörsen“, Neuwied; Kriftel; Berlin: Luchterhand, 1997

[Lut98] Lutterbeck, Bernd: „Geldökonomie, Onlineökonomie und die Sicherheit des Zahlungsverkehrs: Die Fragen der Ersten Generation“; Statement zum BSI-Diskurs Bonn, 5.2.1998

[Lyn97] Lynch, Daniel C. / Lundquist, Leslie: „Zahlungsverkehr im Internet“; Wien: Carl Hanser Verlag, 1997

[Mau90] Mauch, Willy: „Bessere Kundenkontakte dank Sales Cycle“ in THEXIS 7 (1990) 1, S. 15-18

[Mei96] Meister, Edgar: „Cybergeld als Monopol der Notenbanken vorstellbar“, in: Frankfurter Allgemeine Zeitung, vom 29.11.1996, S.19

[mill.com] Millicent Home Page http://www.millicent.digital.com

[MuÖs98] Muther, A. / Österle, H.: „Electronic Customer Care - Neue Wege zum Kunden“; WI-Aufsatz in Wirtschaftsinformatik, Heft 2, 40. Jahrgang, April 1998; S. 105 - 113

[Neu95] Neumann, Horst A.: „Objektorientierte Entwicklung von Software-Systemen“; Addison-Wesley Deutschland, 1995

[KoN93] Kohl, J. / Neumann, C.: „The Kerberos Network Authentifikation Service“, Massachusetts Institute of Technology, 1993

[Nie98] Niehoff, Wilhelm: „Sicherheit im Elektronischen Zahlungsverkehr aus Sicht der Banken“; BSI-Diskurs Bonn, 5.2.1998

[O'Mah97] O'Mahony, Donal / Peirce, Michael / Tewari, Hitesh: „Electronic payment systems“; Artech House, Norwood, 1997

[O'Nei98] O'Neill, Peter: „Der Marktplatz da draußen“; in Internetworld, Februar 1998; S. 44-47

[OII97] „Electronic Payment Mechanisms“; update November 1997; http://www2.echo.lu/oii/en;

[OTP98] „Internet Open Trading Protocol - Part 1: Business Description“; Version 0.9 vom 12. Januar 1998
http://www.otp.org/OTP/Home.nsf

[Patz96] Patzlaff, Rainer: „CyberSpace und die Ich- und Sinnesorganisation des Menschen“; in *Cyber Space, Virtual Reality: Fortschritt und Gefahr einer innovativen Technologie*; hrsg. Von F. Wedde; Stuttgart 1996

[Pern97] Pernul, G. / Röhm, A.: „Neuer Markt - neues Geld?“, WI-Aufsatz; in Wirtschaftsinformatik 39 (1997) 4, S. 345-355

[Pfeff96] Pfeffer, Christine: „Authentifizierung und Zertifizierung im elektronischen Zahlungsverkehr“, Diplomarbeit am Lehrstuhl Informationswissenschaft, Universität Konstanz; Dez. 1996

[Pfi98] Pfitzmann, Andreas: „Hundert Geldsysteme im elektronischen Portemonnaie?“; BSI-Diskurs Bonn, 5.2.1998

[Post91] Postmann, Neil: „Das Technopol - Die Macht der Technologien und die Entmündigung der Gesellschaft“, Verlag S. Fischer, Frankfurt/M, 1992

[Rie98] Riehm, Ulrich: „Banken als Innovationsmotor und -bremse“; in EZI-N Elektronische Zahlungssysteme im Internet, Newsletter - Nr. 11 - 27.3.1998; http://www.itas.fzk.de/deu/projekt/pez/ezin.htm

[Rum93] Rumbaugh, J. / Blaha, M. / Premerlani, W. / Eddy, F. / Lorensen W.: “Objektorientiertes Modellieren und Entwerfen“; Coedition von Hanser und Prentice Hall; London 1993

[SaLB.de] „edd - Das lastschriftbasierte Zahlungssystem von CyberCash“; http://www.sachsenlb.de

[Schi95] Schieber, Peter: „Informationsmanagement II - Strategische Informationsplanung und Business Reengineering“; Bericht 68-95; Konstanz, März 1995

[Schm10/97] Schmid, Beat: „Electronic Commerce: Per Knopfdruck Geschäfte machen“; in Gablers Magazin, Nr. 10/1997; Th. Gabler Verlag, Wiesbaden, Oktober 1997

[Schm2/97] Schmid, Beat / Lindemann Markus: „Elemente eines Referenzmodells Elektronischer Märkte“; Sonderdruck WI-Konferenz, Berlin, Februar 1997

[Schn93] Schneider, Dieter: „Betriebswirtschaftslehre“; Band 1, Grundlagen; R. Oldenbourg Verlag, München, 1993

[Schn97] Schneider, Dieter: „Betriebswirtschaftslehre“; Band 3, Theorie der Unternehmung; R. Oldenbourg Verlag, München, 1997

[Schu3/98] Schumacher, Lutz: „Elektronisch Zahlen“; in internet world, Ausgabe März 1998, S. 61-62

[Schu5/98] Schumacher, Lutz: „Geldgeschäfte“ Interview mit Andrej Ankerst, kfm. Projektleiter CyberCash bei der Dresdner Bank; in internet world, Ausgabe Mai 1998, S. 42-44

[Schu97] Schuster, R. / Färber, J. / Eberl, M.: „Digital Cash: Zahlungssysteme im Internet“; Springer Verlag, Berlin, Heidelberg; 1997

[Sie92] Siefkes, Dirk: “Formale Methoden und kleine Systeme : lernen, leben und arbeiten in formalen Umgebungen“; Braunschweig; Wiesbaden : Vieweg, 1992

[Siet97] Sietmann, Richard: „Electronic Cash : der Zahlungsverkehr im Internet“; Schäffer-Poeschel; Stuttgart, 1997

[Som95] Sommerville, Ian: „Software Engineering“; Lancaster University; Addison Wesley, Fifth Edition 1995

[spie19/1/98] „T-Online auf Wachstumskurs“; o. V.;19. Januar 1998; http://www.spiegel.de/netzwelt:

[spie30/3/98] „T-Online“; o. V.; 30. März 1998; http://www.spiegel.de/netzwelt:

[Stol97] Stolpmann, Markus: „Elektronisches Geld im Internet : Grundlagen, Konzepte, Perspektiven“; O’Reilly Verlag, Köln, 1997

[Sul97] Sullivan, Eamonn: „Outsource the Commerce in E-Commerce“; in ZDNet, PC Week, vom 8. Dezember 1997 http://www.zdnet.com/pcweek

[Ulr98] Ulrich, Dr. Otto: „Paradigmenwechsel unserer Geldsysteme? Zum Stellenwert der Technikfolgenabschätzung in der IT-Sicherheit“; BSI-Diskurs Bonn, 5.2.1998

[useit.com] Nielsen, Jakob: „The Case for Micropayments“, 25. Januar 1998; http://www.useit.com/alertbox/980125.htm;

[Vah97] Vahrenkamp, Richard: „Zahlungssysteme im Internet“; in Informationsmanagement 1/97; Januar 1997; S. 43-49

[Was97] Wasmeier, Michael: „Shop in the Box - Funktionsweise von Online-Shop-Komplettpaketen“; in c’t 07/97, S. 268

[Weis98] Weis, Rüdiger: „Mit Bits bezahlen - Banken prägen Software-Geld“; in PC Magazin, Ausgabe März 1998, S. 234-236

[Wic98] Wicke, Guntram: „Stellungnahme zu EZI-L EZI-N 09“; 13.3.98 http://www.itas.fzk.de/deu/projekt/pez

[Zbo96] Zbornik, Stefan: „Elektronische Märkte, elektronische Hierarchien und elektronische Netzwerke“; Schriften zur Informationswissenschaft, Bd. 22; Univ.-Verlag Konstanz; 1996

[Zeit51’97] Lütge, Gunhild: „Jetzt ist auch in Deutschland der Startschuß für virtuelles Geld im Internet gefallen“; in Die Zeit Nr. 51, vom 12.12.1997, Seite 33

[Zimm97] Zimmermann, Hans-Dieter: „Electronic Commerce heute - Eine kritische Bestandsaufnahme“; Zürich, 19. November 1997

[Zoch98] Zoche, Peter: „Folgen unzureichender oder fehlender IT-Sicherheitsvorkehrungen im elektronischen Zahlungsverkehr - Ausgewählte Projektergebnisse“; BSI-Diskurs Bonn, 5.2.1998