Analyse und Bewertung von elektronischen Zahlungssystemen

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

Bericht-Nr.: BusinessMedia/52
Version: 1.0
Datum: Oktober 1996

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

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

Inhaltsverzeichnis

EUREKA

EUREKA Projekt Nr. 1483
KTI-Projekt Nr. 3245.2

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

Vorwort

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

Der vorliegende Bericht dokumentiert die Ergebnisse des Arbeitspakets Nr. 2 gemäss Projektplan.

Die folgende Tabelle enthält die Projektpartner und deren Repräsentanten:

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

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

1 Einführung

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

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

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

Abgeleitet aus den Anforderungen [Himmelspach et al. 1996] werden zu Beginn technische, betriebswirtschaftliche und nutzerbezogene Beurteilungskriterien für elektronische Zahlungssysteme aufgestellt. Anschliessend werden die Zahlungskategorien elektronische Münzen, Kreditkarten, elektronische Schecks, Smartcards und Zahlungssysteme auf EDI-Basis erläutert. Anhand konkreter Systeme und Produkte wird detailliert auf Vor- und Nachteile, Grundcharakteristika, Marktpotentiale und Probleme eingegangen. Danach folgt die Bewertung ausgewählter Systeme aufgrund der zuvor aufgestellten Beurteilungskriterien. Abschliessend wird noch auf Zahlungsprotokolle eingegangen. Ebenso wie bei den Zahlungssystemen werden Marktpotential und Grundcharakteristika untersucht und im Hinblick auf die Integration in das generische Zahlungssystem beurteilt. Die vorliegende Analyse wurde im Sommer 1996 begonnen und im Herbst 1996 abgeschlossen.

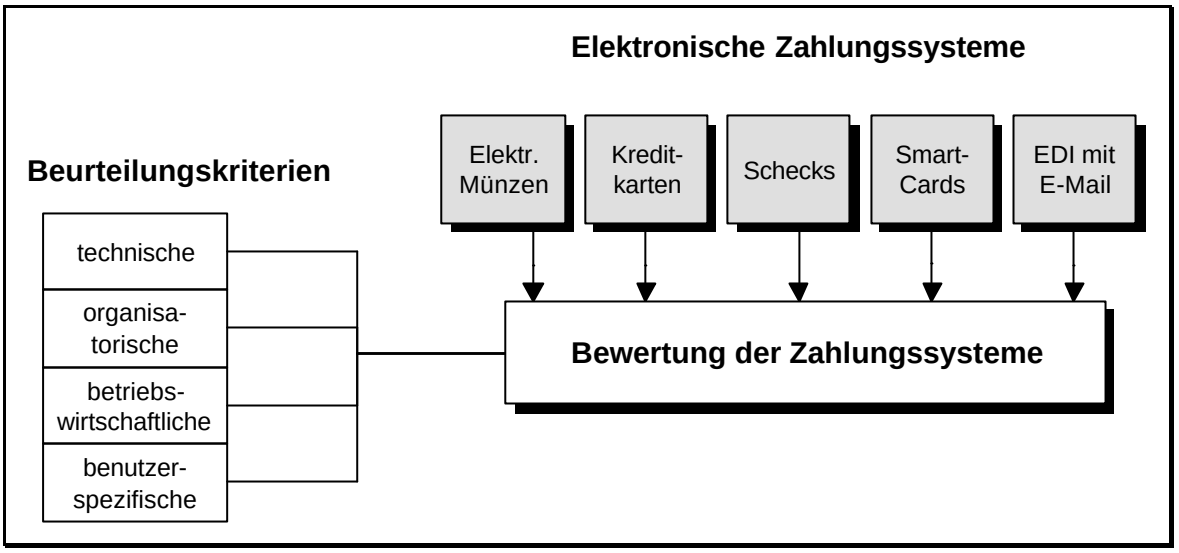

Abbildung 1.1: Überblick

2 Beurteilungskriterien für Zahlungssysteme

Um einen Rahmen zur Einordnung von Zahlungssystemen zu erhalten, müssen Bewertungskriterien aufgestellt werden. Die nachfolgenden Kriterien und Untersuchungen ergeben sich aus den Anforderungen an Zahlungssysteme. Dabei findet eine Gliederung in technische, organisatorische, betriebswirtschaftliche und nutzerbezogene Beurteilungskriterien statt.

Technische Beurteilungskriterien

Die technischen Kriterien beinhalten einerseits die Verschlüsselungsverfahren und die Sicherheitsmechanismen. Weiterhin werden Vertraulichkeit, Integrität, Authentifizierung, Autorisierung, Non-Repudiation und die Verhinderung von Attacken als technische Beurteilungskriterien für elektronische Zahlungssysteme festgehalten. Bei der technischen Realisierung und der Integration sind folgende Kriterien Beurteilungsgegenstand elektronischer Zahlungssysteme: Wahl der Zahlungskommunikation, Durchgängigkeit der IT-Mittel, Integrationsfähigkeit in die Marktplattform, Notwendigkeit zusätzlicher Hardware und die Nutzung des Systems mit Internet-Diensten.

Organisatorische Beurteilungskriterien

Die Abhängigkeiten der Teilnehmer in Bezug auf den Leistungsaustausch (Bezahlung vor Lieferung vs. Lieferung vor Bezahlung), Systemoffenheit und ein möglicher Geldverlust werden als organisatorische Beurteilungskriterien aufgenommen.

Betriebswirtschaftliche Beurteilungskriterien

Als betriebswirtschaftliche Beurteilungskriterien gelten die Aufwendungen (Transaktionskosten und monatliche Gebühren), Zeitpunkt und Art der Zahlung, Währungsvielfalt, Übertragbarkeit des Geldes, Entwicklungspotential (u.a. Akzeptanzstellen) und Eignung für verschiedene Zahlungen.

Benutzerspezifische Beurteilungskriterien

Die Akzeptanz und das Vertrauen sind die Kriterien, die aus Benutzersicht besondere Bedeutung haben. Die für die Kunden wichtige Anforderung der Anonymität fließt ebenso als benutzerspezifisches Beurteilungskriterium mit ein. Weitere Kriterien sind die Risiken der Teilnehmer und die Informationsbereitstellung und Unterstützung durch den Systemanbieter.

Nachfolgende Untersuchung verschiedener Zahlungssystem-Kategorien und Produkte wird später in einer Bewertung zusammengefaßt. Grundlage für die Bewertung sind die aufgestellten Beurteilungskriterien, wobei nicht alle in die Bewertung eingehen.

3 Zahlungssysteme auf Basis elektronischer Münzen

In diesem Kapitel wird zunächst auf die Eigenschaften von Zahlungssystemen eingegangen, die auf elektronischen Münzen basieren. Anhand von Fakten, Grundcharakteristik, Marktreife und Zahlungsprozess werden die Produkte Ecash und NetCash untersucht. Die Bewertung beider Produkte findet später statt.

3.1 Allgemeines

Zahlungssysteme auf Basis elektronischer Münzen bieten dem Benutzer eine hohe Flexibilität und Sicherheit. Münzen, die durch Dateien dargestellt werden [Beutelspacher91, 153ff] sind in kleinen Einheiten vorhanden und ermöglichen ökonomischen Kauf von Gütern, deren Preis im Micropayment-Bereich liegt. Sie sind mit den SmartCards gleichzusetzen, da sie ebenso wie diese ein Höchstmaß an Anonymität bieten [Frotscher95]. Der Konsument kann durch die Nutzung von Zahlungssystemen auf Basis elektronischer Münzen auch gegenüber dem Finanzintermediär anonym bleiben. Im Gegensatz zu anderen Zahlungssystemen werden die elektronischen Münzen und nicht die Konsumenten authentifiziert.

Generell enthält die Datei einer elektronische Münze folgende Informationen:

- Seriennummer (zur Überprüfung auf Mehrfachausgaben)
- Geldwert
- Erstellungsort (wenn mehrere Banken für die Münzerstellung autorisiert sind)
- Gültigkeitsdatum (bestimmt den spätesten Zeitpunkt der Münzeinlösung)
- Zeitstempel (entspricht dem Erstellungsdatum)

Der Konsument kann diese Dateien mit einen WWW-Server oder der speziellen Zahlungssoftware über das Internet von der Bank oder einem Währungsserver herunterladen. Danach speichert er sie auf dem eigenen Rechner, bis er sie zum Kauf verwendet.

Nachteil von diesen Zahlungssystemen ist das Problem der prinzipiellen Duplizierbarkeit von elektronischen Münzen und die daraus resultierende aufwendige Münzüberprüfung, wie sie in [Beutelspacher/Hueske/Pfau93] und [Chaum87] ausführlich diskutiert wird.

3.2 Ecash von Digicash

Name des Zahlungssystems	Ecash
Entwickler	Dr. David Chaum (DigiCash, Niederlande)
Prototyp/Test seit	Oktober 1994 bis Oktober 1995[1]
Einführung am	23. Oktober 1995 (Mark Twain Bank, USA)[2]
Grundcharakteristik	Das Zahlungssystem kreiert digitale Münzen. Es ist aufgrund der angewandten Kryptographie und der von Chaum entwickelten und patentierten „Blind Signature"-Lösung sicher und anonym [Chaum92], [Chaum87], [Cameron95, 231]. Das Geld kann in angeschlossenen Shops ausgegeben werden. Funktionalitäten von Ecash: • Geld von der Bank abheben und dort deponieren • Kontoauszug über ausgeführte und erhaltene Zahlungen • Zahlungsaufträge erstellen • Zahlungsbestätigungen ausführen • Automatisierung von Zahlungsbestätigungen Durch die Entwicklung von Ecash in den Niederlanden fällt das Produkt nicht unter Exportbeschränkungen.
praktischer Einsatz/ Marktreife	Innerhalb der USA ist die Mark Twain Bank als bisher einzige US-Bank in Ecash involviert. Die Resonanz ist nicht so hoch wie dies von der Mark Twain Bank erwartet wurde. Lediglich 50 Anbieter und 1000 Konsumenten (Stand Juni 1996) aus insgesamt 30 Ländern haben ein Konto eröffnet, um Shopping mit Ecash zu betreiben[3]. In Europa wird es vom Internet-Provider EUnet und der Merita Bank[4] in Finnland, die ihren Kunden auch Homebanking über das Internet anbietet, seit März 1996 im Rahmen eines Pilotprojekts getestet[5]. Die Deutsche Bank wird Ende des Jahres 1996 einen Pilotversuch von voraussichtlich sechs Monaten Dauer starten[6]. Der Versuch ist auf Kunden der Deutschen Bank begrenzt, eine Konvertibilität zur Ecash-Währung der Mark Twain und Merita Bank sind nicht gegeben. Teilnehmergebühren fallen keine an. Die Begrenzung der lokalen Geldmenge ist auf DM 400,00 festgesetzt [Deutsche Bank96]. Am 29. November 1995 gewann Ecash zusammen mit zwei anderen Produkten den ersten Preis des „Information Technology European Awards '95", einem jährlichen Wettkampf für innovative IT-Produkte

[1] siehe *Ecash Trial is Now Worldwide*, 06.01.1995, http://www.digicash.com/ecash/trial.html und http://www.digicash.com/publish/ec_pres2.html

[2] siehe *First Bank to Launch Electronic Cash*, 23.10.1995, http://www.digicash.com/publish/ec_pres3.html

[3] vgl. o.V. *Electronic Cash kommt langsam in Fahrt*, online aktuell, Nr. 13, 27.06.96

[4] Homepage-URL der Merita Bank: http://www.merita.fi/

[5] siehe *First European Electronic Cash System Opens for Business on the Internet*, 13.03.1996, http://www.digicash.com/publish/ec_pres4.html,

[6] siehe *Deutsche Bank to Test 'E-Cash' With DigiCash in Pilot Project*, Kimberley A. Strassel, 07.05.1996 und [Christ96], der im Rahmen des Pilotprojektes der Deutschen Bank mit Ecash auf deren Unternehmensstrategie „Bank 2000" verweist, in der die Deutsche Bank als Zielsetzung die Marktführerschaft von elektronischem Geld im Internet ankündigt.

	in Brüssel. Seit März 1996 hat Digicash eine Niederlassung in Australien[7].
Probleme	• keine Multibanken-Fähigkeit • Geldverlust durch Festplatten-Crash (kann z.B. durch Sicherheitskopien der Münzdateien auf Disketten verhindert werden) • keine Stornierung ausgeführter Zahlungen möglich • produktbezogene Zahlung; kein Warenkorb möglich
URL	http://www.digicash.com/

Tabelle 1: Ecash-Fakten

Für die Teilnahme an Ecash müssen die Konsumenten und Verkäufer ein Konto bei einer teilnehmenden Bank eröffnen. Der Prozeß einer Konteneröffnung bei der Mark Twain Bank[8] wird auf der folgenden WWW-Seite beschrieben:

http://www.marktwain.com/digiapp.html

Kunde und Anbieter müssen dabei zunächst die Teilnahmebedingungen der Mark Twain Bank akzeptieren, indem sie das Formular ausdrucken, unterschreiben und per gewöhnlicher Post an die US Bank schicken (siehe Abbildung 2.2). Dort wird ein Konto eingerichtet, was den Kunden zwischen US$ 11,00 und US$ 25,00 und den Anbieter zwischen US$ 150,00 und US$ 500,00 je nach gewünschter Nutzungsintensität kostet. Nachdem die Mark Twain Bank die Software per übersandtem Paßwort zur Verfügung gestellt hat, findet ein zweiter Medienbruch bei der Registrierung statt: die Überweisung der SetUp-Gebühr (zuzüglich Guthaben bei Kunden) per gewöhnlichem Zahlungsmittel. Für ein Guthaben über US$ 2.500,00 erhält der Kunde eine Zinsgutschrift[9].

Für den Anbieter beginnt nach dem Laden der Software die Shop-Installation, d.h. er muß seine immateriellen Produkte, die er über das Internet vertreiben möchte, in bestimmte Verzeichnisse kopieren und für diese Verzeichnisse Zugriffsrechte vergeben. Weitere Informationen zur Einrichtung von Ecash-Shops, die u.a. die Shop-Installation bei dem Verkauf von materiellen Gütern beschreiben sind ersichtlich auf der Page:

http://www.digicash.com/ecash/ecash-issuers.html

Nachfolgend wird die Konteneröffnung von Kunden und Anbietern bei der Mark Twain Bank skizziert:

[7] siehe *DigiCash Opens for Business in Australia*, 26.03.1996,http://www.digicash.com/publish/austra.html
[8] vgl. http://www.marktwain.com/digiapp.html
[9] vgl. http://www.marktwain.com/fee.html

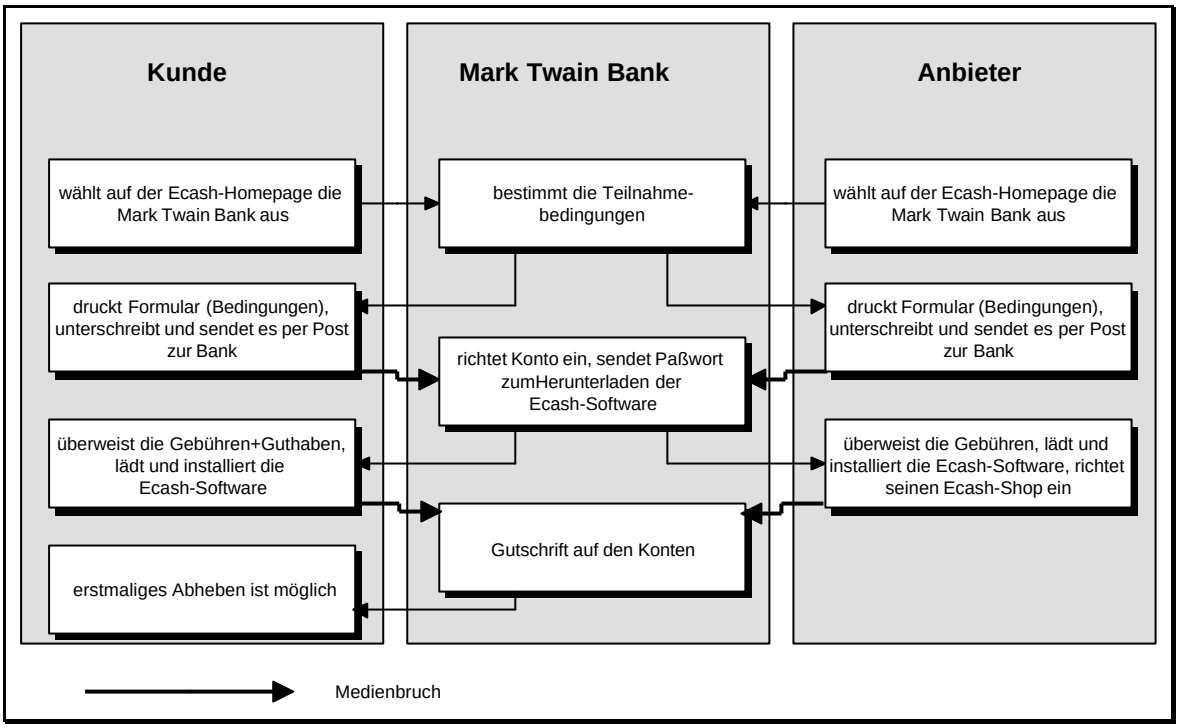

Abbildung 3.2: Kontoeröffnungsprozeß bei Ecash

Bevor der Kunde mit dem Einkaufen beginnen kann, muß er Geld von seinem Konto bei der Mark Twain Bank auf seinen lokalen Rechner herunterladen. Bei diesem erstmaligen Herunterladen werden von der Ecash-Software die Kryptographieschlüssel generiert und ein Paßwort (notwendig für Geldabhebung bei der Bank) muß angegeben werden.

Danach kann der Kunde in einem Ecash-Shop, welcher der Mark Twain Bank angeschlossen ist, ein Produkt auswählen, womit er eine Zahlungsstransaktion startet (siehe Abbildung 2.3). Durch die Produktauswahl wird von der bereits gestarteten Ecash-Software beim Kunden eine Zahlungsaufforderung kreiert, die per Mausklick bestätigt werden muß. Voraussetzung ist, daß der Kunde seine Ecash-Software bereits gestartet hat.

Wird die Zahlungsaufforderung mit „Ja“ bestätigt, sendet die Software die verschlüsselten elektronischen Münzen zum Anbieter, der sie unverzüglich zur Mark Twain Bank weiterleitet. Dort wird basierend auf der Seriennummer überprüft, ob die gleiche Münze bereits eingelöst wurde. Falls dies nicht zutrifft, wird die Münze in dieser Datenbank gespeichert und der Betrag dem Anbieter gutgeschrieben bzw. neue Münzen erstellt und dem Anbieter übersandt.

Sobald der Anbieter die Nachricht über die Gültigkeit der Münzen erhält, schaltet seine Software das Produkt frei. Ebenso erhält der Kunde eine Quittung, die in Form eines Transaktionssatzes in seiner Ecash-Software gespeichert wird und auf Abruf sichtbar wird. Die Zahlungstransaktion inclusive der Freischaltung des Produkts dauert zirka 15 Sekunden.

Falls der Kunde die Zahlungsaufforderung nicht bestätigt, wird ein HTML-Formular sichtbar, das mögliche Fehler der Zahlungstransaktion beschreibt und mit dem um eine erneute Zahlung gebeten wird. Die Erstellung eines solchen Formulars wird dem Anbieter von DigiCash empfohlen, ist aber optional.

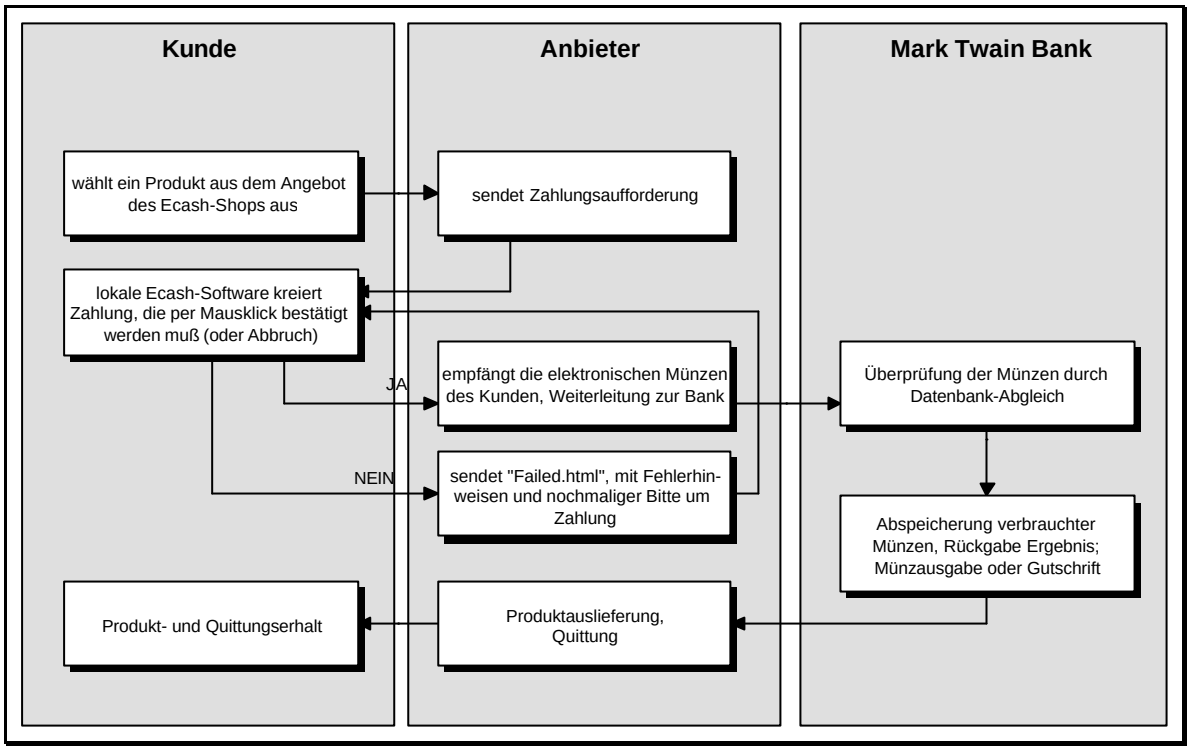

Abbildung 3.3: Zahlungstransaktionsprozeß bei Ecash

Ecash wird, trotz seiner bisherigen Problemen wie fehlende Multibankenfähigkeit und Geldverlust durch Festplatten-Absturz, eine sehr hohe Bedeutung zugemessen. So haben, laut der bereits erwähnten Studie von [Weiler96] bereits im Jahre 1995 rund 27% der Befragten das System benutzt. [Waidner96a] bezeichnet es das Zahlungssystem, das am fortschrittlichsten ist.

Bei DigiCash wird momentan das Problem der Multibankenfähigkeit angegangen; dezentralisierte Datenbanken zur Münzüberprüfung bei den teilnehmenden Banken sind denkbar, Voraussetzung dieser Lösung ist allerdings, daß alle Banken stets online sind (Online-Verifizierung der Münzen), damit das Gesamtsystem funktionsfähig ist.

3.3 NetCash von der University of Southern California

Name des Zahlungssystems	NetCash
Entwickler	Information Sciences Institute (ISI) University of Southern California (Clifford Neuman und Gennady Medvinsky)
Prototyp/Test seit	nicht bekannt
Einführung am	voraussichtlich in 1997[10]
Grundcharakteristik	NetCash produziert digitale Münzen, die mit Signaturen der Bank versehen sind. Die Infrastruktur basiert auf unabhängigen, verteilten Währungs-Servern (WS) und mehreren Accounting-Servern (AS). Aufgaben der Währungs-Server [vergl. Frotscher95]: • Überprüfung der Münzen auf Echtheit • Münzaustausch gegen neue Münzen gleichen Wertes, um die Verfolgung der Münzen zu verhindern und somit die Anonymität der Besitzer zu wahren • Verkaufen und Einlösen von Münzen Aufgaben der Accounting Server: • führen die WS-Konten, • führen die Konsumenten-Konten, • lösen Schecks ein • identifizieren bei Scheckeinlösung die WS Die WS werden von einer zentralen Depot- und Versicherungsbehörde überwacht und bekommen von ihnen Erlaubniszertifikate, die sie zur Ausgabe elektronischer Münzen befähigt [Frotscher95].
praktischer Einsatz/ Marktreife	noch in Testphase, kein kommerzieller Einsatz
Probleme	Die eindeutige Seriennummer der Münze ist dem WS bekannt, was ihn dazu befähigt, die überwiesenen und gelagerten Münzen den Kunden zuzuordnen und eine ensprechende Statistik abzuspeichern [Finney93]. Laut Wayner sind die verwendeten Protokolle recht einfach gestaltet, so daß die Banken möglicherweise die Kundenspuren zurückverfolgen können [Wayner96, 123]. Es besteht daher die Möglichkeit, das der Kunde zum „gläsernen Menschen wird“.
URL	http://nii-server.isi.edu:80/info/netcash/

Tabelle 2: NetCash-Fakten

NetCash kann mit dem System NetCheque kombiniert werden. In der Abbildung 2.4 ist ersichtlich, wie das scheckbasierten System NetCheque einer Zahlungstransaktion mit NetCash vorgeschaltet wird, um elektronische Münzen vom WS zu erhalten. Mit NetCash wurde ein Verfahren entwickelt, das den beiderseitigen Schutz der Marktteilnehmer berücksichtigt. Der Mechanismus läßt sich wie folgt beschreiben:

⇒ Der Kunde sendet eine Münze M an der Währungs-Server, der aus dieser Münze mehrere Münzen (M1, M2, M3) mit gleichem Wert und gleicher Seriennummer aber unterschiedlichen Gültigkeitszeiträumen kreiert.

[10] lt. Bob Gassen der CyberSAFE Corportation (http://nii.isi.edu/info/netcash/commercial.html) E-Mail vom 10.07.96

⇒ Nachdem der Kunde beim Anbieter ein Produkt ausgewählt hat, bezahlt er mit M1, die eine bestimmte Gültigkeitsdauer hat.

⇒ Angenommen der Anbieter zahlt die Münze innerhalb des Gültigkeitszeitraumes beim Währungs-Server ein, liefert jedoch nicht das Produkt, kann der Kunde, nachdem der Gültigkeitszeitraum von M1 abgelaufen ist, den Mißbrauch durch Nachfrage beim Währungs-Server aufdecken und eliminieren lassen.

⇒ Der Währungs-Server gibt dem Kunden eine neue Münze mit dem Wert von M1 aus, und belastet sie dem Anbieter-Konto.

Voll ausgereift ist der Mechanismus jedoch nicht, da bisher noch nicht geklärt ist, wie der Kunde beweisen soll, daß er tatsächlich keinen Gegenwert für die Münze M1 von dem Anbieter erhalten hat [Frotscher95].

Der Mechanismus des beiderseitigen Schutzes bei Zahlungstransaktionen über das Internet ist in der unten aufgeführten Abbildung nochmals zusammenfassend dargestellt.

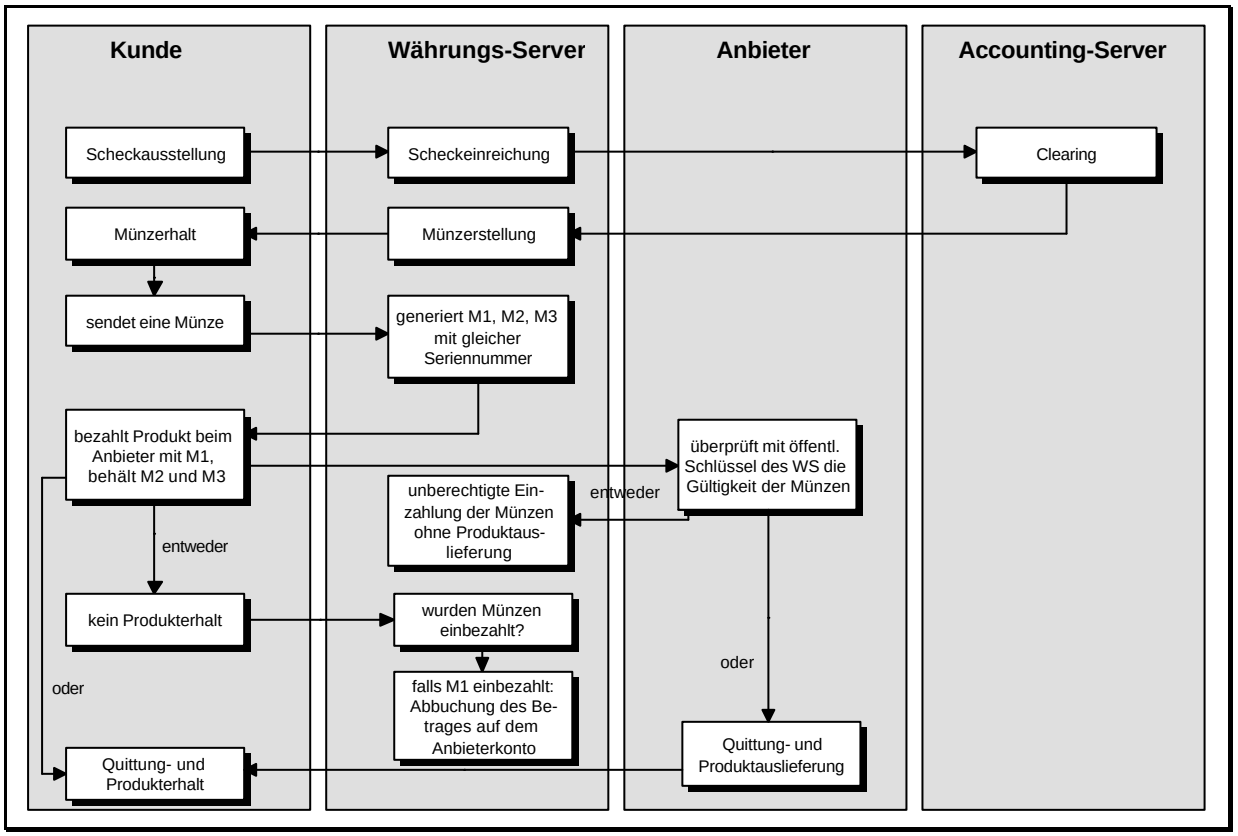

Abbildung 3.4: Zahlungstransaktionsprozeß bei NetCash

Ob sich das System nach seiner kommerziellen Einführung im Jahre 1997 durchsetzen wird, bleibt abzuwarten. Jedoch sprechen die kombinierte Nutzung mit NetCheque, die Offenheit des Systems (mehrere WS und AS) und die Eignung für Micropayments für die Verbreitung und den erfolgreichen Einsatz.

3.4 Cybercoin von Cybercash[11]

Name des Zahlungssystems	Cybercoin
Entwickler	Cybercash
Prototyp/Test seit	September 1996 (Maze.com)
Einführung am	Oktober 1996 (Cybercash, USA)
Grundcharakteristik	Das Zahlungssystem kreiert Zertifikate für digitale Münzen Kryptographie: RSA 1024, DES 56 Bits. Das System ist privat, aber nicht anonym, wobei die Kreditkarteninformationen bzw. Bankinformationen dem Anbieter verborgen bleiben. Das Geld kann in registrierten Shops ausgegeben werden, welche bei Cybercoin angeschlossen sind. Funktionalitäten von Cybercoin: • Geldausgabe via Kreditkarte oder Bankkonto • Kontoauszug über ausgeführte und erhaltene Zahlungen im Wallet • Automatisierung von Zahlungsbestätigungen • relativ hohe Transaktionskosten (mindestens 2.5%) • Multibankenfähigkeit (Oktober 96: 10 Finanzinstitutionen) Durch die Entwicklung in den USA fällt das Produkt unter Exportbeschränkungen, allerdings existiert eine Ausfuhrgenehmigung.
praktischer Einsatz/ Marktreife	Da das Produkt noch relativ neu ist, sind erst wenige Händler und Banken angeschlossen. Es kann allerdings erwartet werden, dass alle bisherigen Partner von Cybercash auch das neue Produkt nutzen werden. Es ist eine Kooperation mit einem Internet Content Provider in Norwegen geplant. Ausserdem gibt es Kooperationsvereinbarungen mit Oracle, Sun und Netscape.[12] Oracle beabsichtigt die Produktpalette in ihren Webserver einzubauen. Nebst Cybercash/-coin soll auch ein elektronisches Checksystem integriert werden. Netscape baut in zukünftige Versionen ihrer Produkte die Technologie ein. Es ist die Absicht vorhanden, die Produktfamilie in bestehende Finanznetze zu integrieren. Cybercoin könnte eine wichtige Bedeutung haben im Bereich von Pay per view Applikationen und billigen Soft-Goods.
Probleme	• keine Stornierung ausgeführter Zahlungen möglich • produktbezogene Zahlung; kein Warenkorb möglich • Maximalbetrag von 100$
URL	http://www.cybercash.com/

Tabelle 3: Cybercoin-Fakten

Für die Teilnahme an Cybercoin müssen die Konsumenten und Verkäufer ein Konto bei Cybercoin eröffnen. Der Prozess einer Kontoeröffnung (und Installation des Cybercoin Wallets) erfolgt benutzergeführt. Das Wallet kann auf den Rechner geladen werden unter der URL: ftp://ftp.cybercash.com/pub/wallet/win.

[11] Http.//www.cybercash.com

[12] Newslist: E.C TODAY - v 96.10.11, v 96.12.10 -, vnetwork @ nbnet.nb.ca

Nachfrager.
Die Teilnahmebedingungen und die bankrechtlichen Vorschriften werden bei der Installation der Software bestätigt. Die Registrierung mit allen Passwörtern geschieht online, ohne Medienbruch. Allerdings können in der Anfangsphase die Informationen zu den Kreditkarten noch nicht online, sondern via Fax oder E-Mail übermittelt werden. Für den Kunden fallen keine Set-up Gebühren an, der Kontostand ist aber generell auf 100$ beschränkt.

Anbieter.
Die Shop-Installation beginnt für den Anbieter mit der Bereitstellung elektronischer Güter. Ohne Erlaubnis der Bank erhält der Händler kriegt keine Kreditkarteninformationen oder andere persönliche Daten.

Nachfolgend wird das Einrichten der Konti für Anbieter und Kunden skizziert.

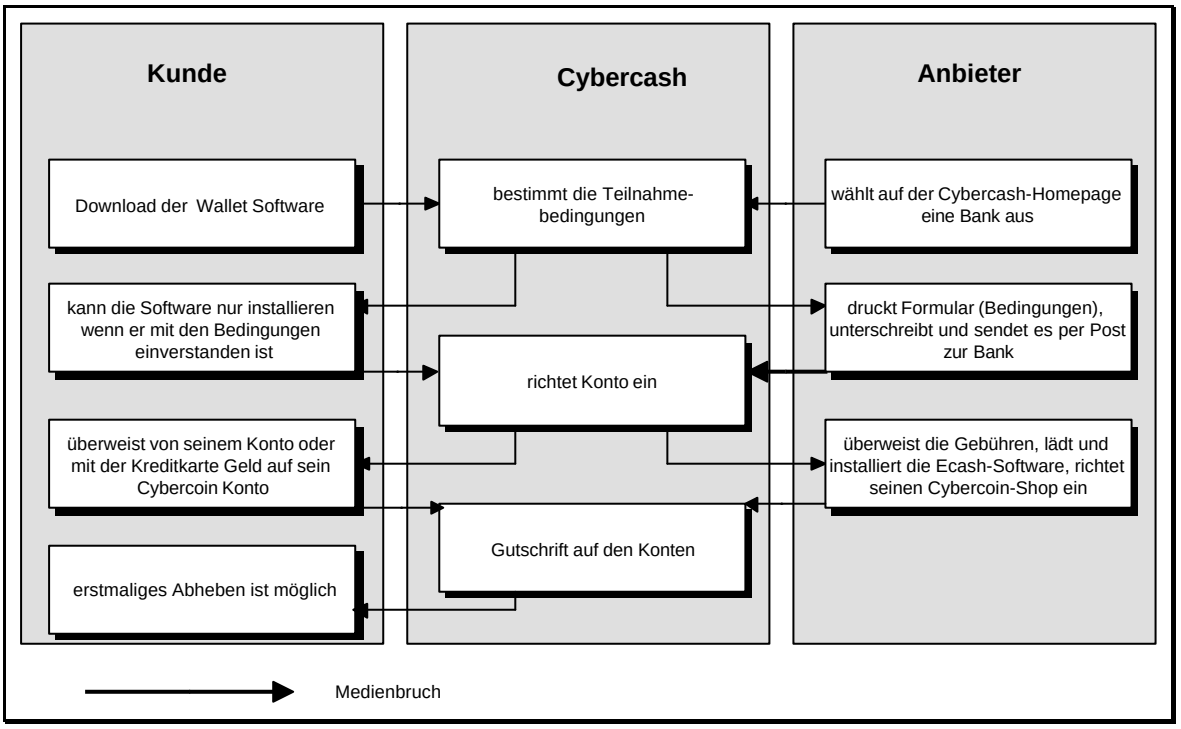

Abbildung 3.5: Set-Up bei Cybercoin

Bevor der Kunde mit dem Einkaufen beginnen kann, muß er Cybercoins herstellen. Dies kann einerseits via Kreditkarte bei einer Partner-Bank oder mittels einer Überweisung auf ein Cybercash Konto geschehen. Mit dem Wallet von Cybercash können dann Coins produziert werden. Mit der Software werden die Zertifikate für Münzen auf dem Rechner gespeichert. Die Installation der Software verlangt auch einen Identifikations-Schlüssel, mit welchem bei Verlust der Zertifikate (bei Datenverlusten, wie Harddisk-Crash), neue Münzen generiert werden können.

Danach kann der Kunde in einem Cybercoin-Shop ein Produkt auswählen. Die ausgewählte Datei wird auf den lokalen Rechner verschlüsselt gespeichert, oder es wird ihm der Zugriff auf eine Seite gewährt. Zusätzlich werden noch zwei Dateien übertragen, mit welchen die gewünschte Datei, mit

den zusätzlichen Informationen, die bei der Zahlungstransaktion übermittelt werden, dechiffriert werden kann.

Wird die Zahlungsaufforderung bestätigt, werden die Beträge dem Anbieter gutgeschrieben. Es findet eine zentrale Überprüfung der Zertifikate statt und bei einer positiven Rückmeldung wird die Transaktion ausgelöst. Der Betrag wird dem Wallet des Anbieters gutgeschrieben, welcher von Zeit zu Zeit den Betrag auf seinem Bankkonto gutschreiben lassen kann. Die Transaktion wird aufgezeichnet, wodurch der Kunde jederzeit mittels der Software die Transaktionen rekonstruieren kann.

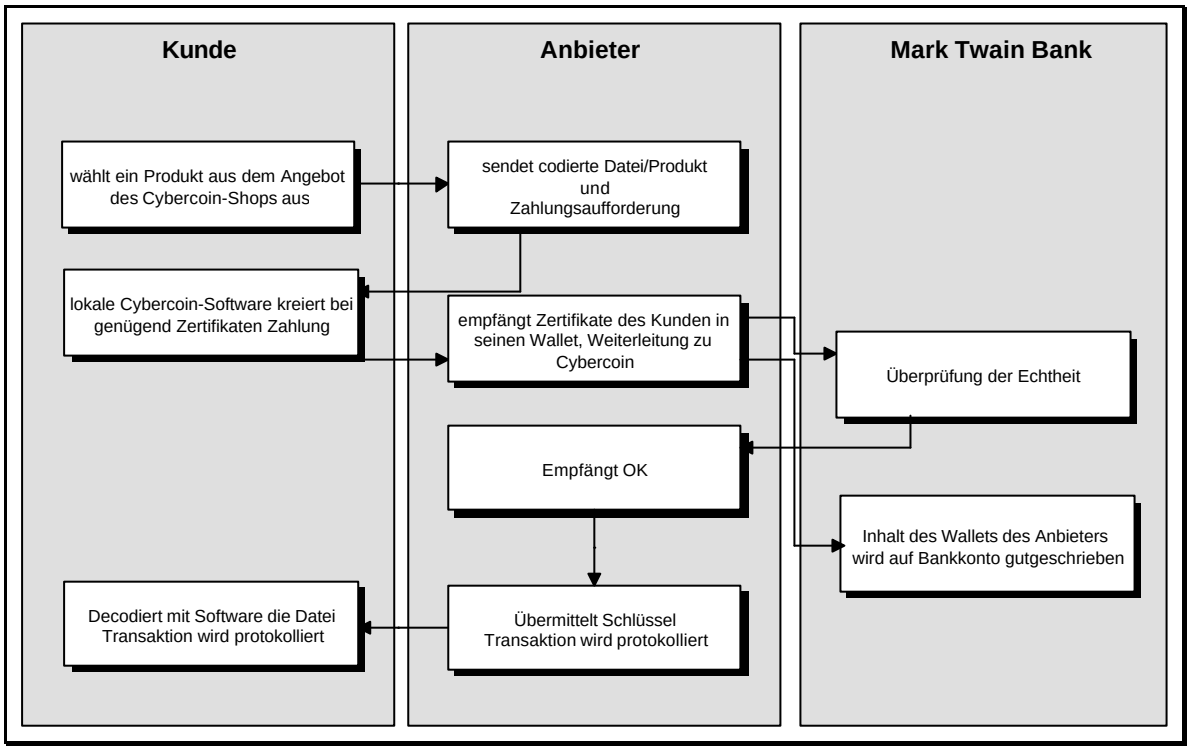

Abbildung 3.6: Zahlungstransaktionsprozeß bei Cybercoin

Beurteilung.
Vor allem durch die offene Struktur sowie die Multibankenfähigkeit könnte Cybercoin eine Rolle im Bereich der Micro-Payments spielen.

Nachteil ist, dass bei jeder Transaktion eine Verifizierung der Münzen auf einem Server von Cybercoin statt findet, was zu grossen, zeitlich aufwendigen Netzbelastungen führt.

Ein Problem für den Anbieter liegt darin, dass das gekauft Produkt zuerst auf den lokalen Rechner geladen wird und erst im Anschluss an die Datenübermittlung bezahlt wird. Die Produkte werden nach der Bezahlung decodiert. Dieses Prozedere ist mit Vor- und Nachteilen behaftet. Stellt sich während der Datenübermittlung ein Unterbruch ein, hat der Kunde nicht bezahlt, hat das Produkt aber in chiffrierter Form erhalten. Dies ist problematisch, da der Schlüssel zum Decodieren der Nachricht in einer lokalen Datei vorhanden ist. Mit dem entsprechenden Know-how könnte die Datei mit einer einfacher Software decodiert werden.

3.5 Millicent von Digital Equipment[13]

Name des Zahlungssystems	Millicent
Entwickler	Digital Equipment
Prototyp seit	September 1996
Einführung am	bis jetzt kein kommerzieller Einsatz
Grundcharakteristik	Das System von Millicent versucht die Transaktionskosten und die Geschwindigkeit, die durch die Netznutzung entstehen, massiv zu verkürzen. Erst tiefe Kosten erlauben auch wirtschaftliche Zahlungen im Cent-, resp Subcent-Bereich. Ein weiteres Merkmal sind die einfachen Verschlüsselungsmechanismen welche dieses System benutzt. Das Knacken des Systems ist aufwendiger als der Kauf von digitalen Checks, womit auch die einfache verwendete Kryptographie ausreicht. Funktionalitäten von Millicent: • Geld wird via Kreditkarte oder mit Hilfe anderer Zahlungssysteme (Macrocommerce-Instrumente) generiert • Die Zahlungen werden beim Kunden nicht aufgezeichnet • Sehr tiefe Transaktionskosten (0.1 Cent) • Unabhängigkeit von Banken • Schnelle Transaktionsabwicklung bei sich wiederholenden Prozessen Das Produkt fällt nicht unter die Exportbestimmungen der USA, da die Verschlüsselung relativ einfach ist.
praktischer Einsatz/ Marktreife	Das Produkt ist nur für den Bereich der Micropayments gedacht (Beträge kleiner 2 US Dollar). Es ist bisher noch nicht im Markt eingesetzt worden, allerdings sind einige Chancen für einen Erfolg vorhanden. Dies unter anderem, weil Digital Equipment hinter dem Produkt steht. Es stellt sich die Frage, ob eine homogene Produktfamilie für Micro-, Mini-, und Macrocommerce nicht eine höhere Chance im Markt hätte als ein einzelnes Produkt, welches lediglich einen Teilbereich abdeckt. Es ist anzunehmen, dass das System eine Rolle im Bereich von Pay-per-view-, Pay-per-use-Applikationen (Search Engines, virtual Software-house) übernehmen könnte.
Probleme	• keine Stornierung ausgeführter Zahlungen möglich • produktbezogene Zahlung; kein Warenkorb möglich • relativ kompliziertes System für den Benutzer • digitales Geld gilt nur für einen Shop
URL	http://www.research.digital.com/SRC/millicent

Tabelle 4: Millicent-Fakten

Für die Teilnahme an Millicent müssen Verkäufer mit einem Broker einen Vertrag über die Ausgabe von händlerspezifischen Scrips (Millicent-Währung) abschliessen. Will ein Kunde beim Händler etwas einkaufen wird er aufgefordert, beim Broker-Scrips zu kaufen.

[13] Http.//www.research.digital.com/SRC/millicent

Nachfolgend wird die Installation und die Scripgenerierung des Kunden aufgezeigt.

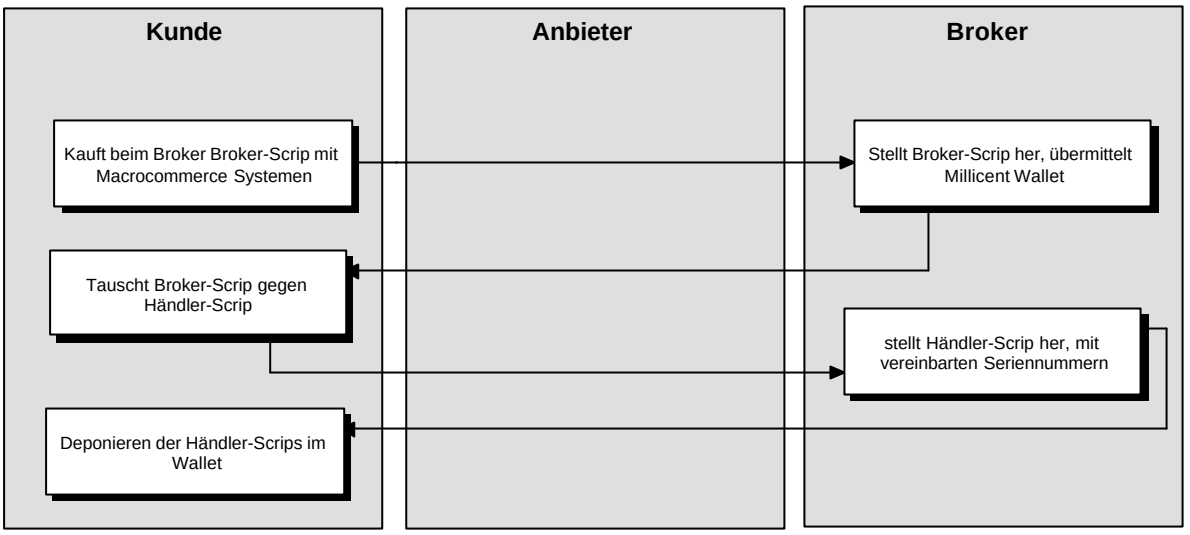

Abbildung 3.7: Set-Up bei Millicent

Bevor der Kunde mit dem Einkaufen beginnen kann, muss er Millicent Scrips kaufen. Dies ist ein zweistufiger Prozess: Zuerst muss beim Broker gegen Kreditkarte (mittels SET, resp. SSL) oder anderen Zahlungsmitteln Broker-Scrip gekauft werden, und der Millicent Wallet lokal installiert werden. In einer zweiten Phase kann Broker-Scrip beim Broker gegen händlerspezifisches Scrip eingetauscht werden. An diesem Punkt ist es dem Broker überlassen welche Informationen des Kunden er in das Scrip einbauen will. Dies können Informationen über Wohnort (Verkaufssteuern etc.) oder Alter und weitere Daten sein, welche für den Händler wichtig sein können. Es liegt an der Seriosität des Brokers und an dessen Kommunikation mit dem Kunden, welche Daten er weitergibt.

Der Kunde kann nun im Shop des Anbieters seine Ware kaufen. Entscheidet sich der Kunde für ein Angebot, wird das Anbieter-Scrip vom Kunden übermittelt. Die Transaktion kann den Präferenzen des Kunden entsprechend entweder mit einem Passwort geschützt, nur bestätigt oder automatisiert werden. Der Anbieter überprüft das Scrip auf seiner lokalen Datenbank (auf welcher die Identifikationsnummern, die mit dem Broker vereinbart wurden, abgespeichert sind) auf seine Gültigkeit. Ist diese gegeben wird die Ware übermittelt, der Betrag vom Scrip abgebucht und in das Wallet des Kunden zurückgesandt.

Ein Teil des Systems ist so konzipiert, dass in gewissen Anwendungen auch ein Bonus für die Benutzung von Seiten gegeben werden kann und diese dann dem Scrip gutgeschrieben werden. So sind auch Rabattsysteme möglich, welche bei mehrmaliger Nutzung Informationen auf einer Folgeseite übermitteln können. Im Scrip selbst können auch Rabattkategorien (z.B. Studenten) eingebunden werden, welche dann gewisse Seiten billiger erhalten.

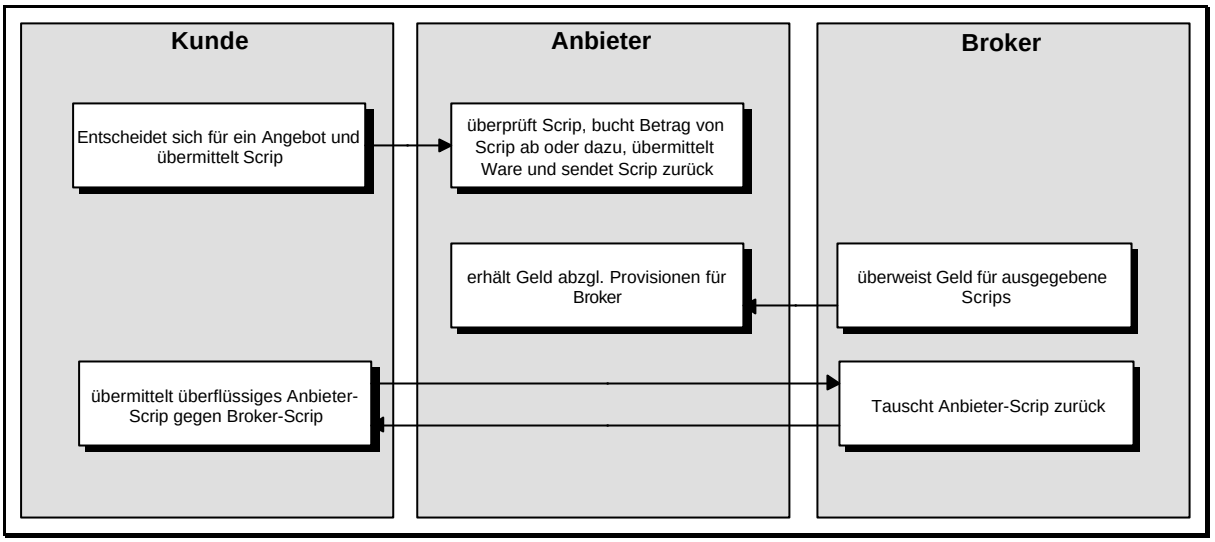

Abbildung 3.8: Zahlungstransaktionsprozeß bei Millicent

Da ein zentraler Validierungsprozess fehlt, ist dieses System relativ schnell. Die Hauptproblematik liegt darin, dass für jeden Shop neue Währung geschaffen werden muss und dies den Kunden verunsichern kann.

Das System ist sehr offen konzipiert, so dass es dem Broker und dem Markt angepasst werden kann vor allem was das Bezahlen der verschiedenen intermediären Dienstleistungen der verschiedenen teilnehmenden Akteure angeht.

Die implementierte geringe Sicherheit, resp. die schwache Verschlüsselung könnte sich nachteilig auf das Kundenvertrauen in das System auswirken. Die Anonymität des Kunden kann durch verschiedene Informationen im Scrip zumindest teilweise verloren gehen (es liegt im Ermessen des Brokers, dies zu verhindern).

4 Zahlungssysteme auf Basis von Kreditkarten

Dieses Kapitel beinhaltet eine Einführung, in welcher allgemeine Aspekte von Kreditkarten-Zahlungssystemen im Internet erläutert werden. Danach folgt die Beschreibung von den Produkten First Virtual und CyberCash. Es wird ein Überblick über die Charakteristik, Marktreife und somit auch die Akzeptanz dieser Systeme gegeben, die nochmals ausführlich bewertet werden.

Weitere, hier nicht erläuterte Kreditkarten-Systeme finden sich auf nachfolgenden Web-Seiten:

http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html
http://www.wiso.gwdg.de/ifbg/geld.html

4.1 Allgemeines

Zahlungen über das Internet wurden bisher überwiegend mit Kreditkarten getätigt [Weiler96] und diese Zahlungsart wird auch in Zukunft dominieren [Weisman/Trevino/Sweet96], da hier internationale Verbreitung (mehr als 800 Millionen Kreditkarten weltweit [Foremski96]) und Standardisierung

vorhanden sind. Der herkömmliche Prozeß der Kreditkartenzahlung wird dabei auf das Internet abgebildet und ein Zahlungs-Server bedient generell die Schnittstelle zwischen dem Internet und dem Finanznetzwerk. Die Bearbeitung von Kreditkartenzahlungen (z.B. das Clearing) ist bisher immer noch zu teuer für Micropayment-Einkäufe. Selbst durch hinzufügen eines Zertifikates bei Kreditkartenzahlungen (Folge:Verringerung der Betrugsrate) und der daraus resultierenden Kostenreduktion ist eine Eigung für Micropayment-Einkäufe nicht zu erreichen.

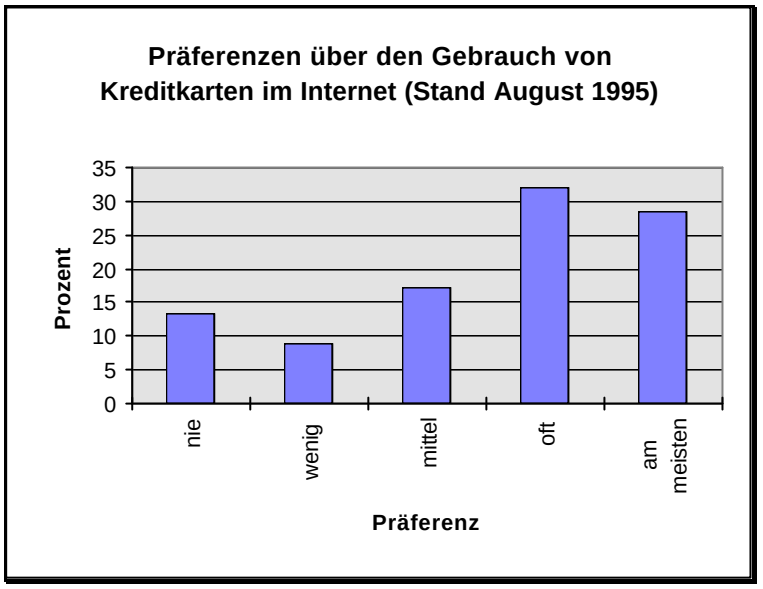

Abbildung 4.9: Präferenzen der Kreditkartenzahlung [Weiler96]

Die Bezahlung mit der Kreditkarte (VISA, MasterCard, Barclays, u.a.) im Internet bietet keine Anonymität, da das Finanzunternehmen sämtliche Daten erhält und speichert, wie dies bei der bisherigen Abrechnung auch außerhalb des Internets der Fall ist. Weiterhin gilt ein Zahlungvorgang erst als genehmigt, wenn innerhalb einer bestimmten Zeit (meistens neunzig Tage) keine Einwände des Kunden gegen die monatliche Kreditkarten-Abrechnung eingebracht wurde [Janson/Waidner96a, 4]. Einen Vorteil bei der Zahlung mit Kreditkarten sehen die Banken darin, daß die Transaktionen bei Kreditinstituten beginnen (Authentifizierung der Kreditkarte) und enden (Gutschrift auf dem Anbieterkonto). Somit entfällt die gefürchtete, unkontrollierte Geldvermehrung durch mehrfachen Geldumschlag innerhalb des Netzes [Raudszus96].

Nachteile treten auf, wenn Kreditkartennummern unverschlüsselt über das Internet übertragen werden, denn mit spezieller Software (Paketsniffern) kann das Internet-Protokoll gezielt abgehört werden [Reif96, 144]. Eine durch das Forschungs- und Beratungsunternehmen Global Concepts in Atlanta erstellte Studie aus 1995, die für VeriFone, VISA und MasterCard erstellt wurde, belegt, daß viele Konsumenten dem Karten-Mißbrauch eine hohe Bedeutung beimessen[14]. Jedoch verwenden fast alle aktuellen Systeme Verschlüsselungsmechanismen. Ein weiterer Schutz vor dem Abhören bietet der immens hohe E-Mail-Aufkommen im Internet. Weiterhin ist ein sichere Speicherung der Kreditkartennummer bei dem Kreditkarteninstitut erforderlich. Ein bekannter Fall von Kreditkarten-Informationsraub ist z.B. der „Einbruch“ einen Rechner von Netcom (Internet-Provider) durch Kevin

[14] vgl. *Money and Concerns found in Internet Commerce*, in Data Storage Report via Dow Jones Retrieval, 01.07.96; Publiziert in: „e-payments“-Diskussionsliste am 07.08.96 von Tom Wills

Mitnick im Jahre 1994. Die Beute war 20.000 Datensätze mit Kreditkarteninformationen [Reif96, 145].

4.2 First Virtual von der First Virtual Holdings Incorporated

Name des Zahlungssystems	First Virtual (FV)
Entwickler[15]	Nathaniel S. Borenstein, Marshall T. Rose, Einar A. Stefferud und Lee Stein (FIRST VIRTUAL Holdings Incorporated)
Prototyp/Test seit	Mai 1994
Einführung am	15. Oktober 1994
Grundcharakteristik	FV ist ein Kreditkarten-Zahlungssystem, welches dem Kunden ermöglicht, das Produkt vor dem Kauf zu testen. Für Zahlungen werden E-Mails verwendet, die auf SMTP/RFC822/MIME und SMXP basieren. Es wird keine Kryptographie angewandt. Für einen Kaufvorgang sind eine große Anzahl von Transaktionsschritten auszuführen, was die Kommunikationskosten in die Höhe treibt. Die Kunden müssen bei FV eine VirtualPIN beantragen und die Anbieter ihre Bankverbindung bekanntgeben. Die Gebühr für eine Zahlungstransaktions-Übersicht beläuft sich für den Kunden auf US$ 2, der Anbieter kann für US$ 1eine Übersicht seiner Einnahmen beziehen. Die Registierung bei FV kostet den Anbieter einmalige US$ 10 , der Kunde muß US$ 2 bezahlen. Die Belastung der Kundenkonten und Gutschrift der Anbieterkonten erfolgt täglich.
praktischer Einsatz/ Marktreife	Laut Garfinkel benutzen mehr als 84.000 Kunden mit über 4.000 Transaktionen pro Woche das System und weit mehr als 1.100 Händler nehmen teil. Die täglichen Geldbewegungen belaufen sich auf US$ 60.000 [Garfinkel96][16].
Probleme	• FV-Zahlungsserver speichert alle Transaktionsdaten • Abhörgefahr, da keine Verschlüsselungen[17] • geschlossenes System • keine Rückerstattungen • produktbezogene Zahlung; kein Warenkorb • keine Stornierung ausgeführter Zahlungen
URL	http://www.fv.com/

Tabelle 5: First Virtual-Fakten

Um bei dem System FV teilnehmen zu können, benötigt der Kunde eine E-Mail Adresse im Internet und eine gültige VISA oder MasterCard Kreditkarte. Ausgehend von der WWW-Seite

[15] Die Entwickler haben First Virtual ganz im Sinne eines verteilten Systems von unterschiedlichen Orten (San Diego, Orange, Silicon Valley und New Jersey) aus entwickelt. Physische Büros gab es erst 15 Monate nach Firmengründung und 8 Monate, nachdem das System lauffähig war. Probleme und Vorteile dieser verteilten Firma sind ausführlich in [Borenstein96] erläutert.

[16] vgl. http://www.fv.com/gabletxt/sjm2_1_29_96.html

[17] Um die Problematik der fehlenden Verschlüsselungen abzuschwächen zeigte die FV Holdings mit einem Programm auf, daß Verschlüsselung allein nicht die Lösung für die garantierte Sicherheit ist, da die Verschlüsselung nicht direkt bei der Eingabe an der Tastatur beginnen kann. Das Programm ist eine Art Bildschirm-Abhörer; es beobachtet die Tastatur und wartet, bis der Benutzer eine komplette Kreditkartennummer eingegeben hat. Theoretisch kann die Nummer an andere Internet-Teilnehmer versendet werden. First Virtual weist mit diesem Programm auf die Sicherheitsproblematik bei Software-Lösungen hin.

http://www.fv.com/info/intro.html

kann die Registrierung gestartet werden. Das Registrierungsformular[18] muß ausgefüllt und per „submit“ an FV gesandt werden. Danach erhält der Kunde seine gültige VirtualPIN, mit der er seine Kreditkartennummer per Telefon an FV durchgibt (siehe Abbildung 3.6).

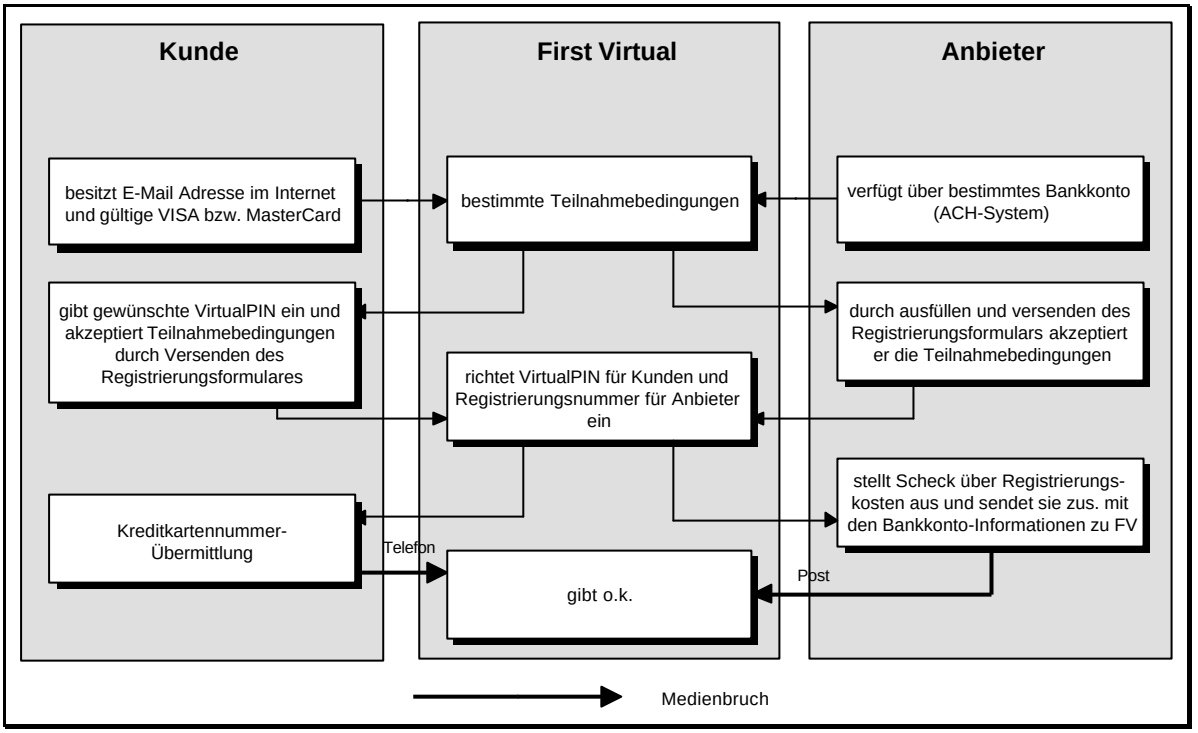

Abbildung 4.10: Registrierungsprozeß bei First Virtual

Bei FV werden die Nummern auf einem separaten Rechner abgespeichert. Mit der VirtualPIN veranlaßt der Kunde nachfolgend die Zahlungen, so daß die Kreditkartennummer nie über das Internet versendet werden muß.

Ein Anbieter muß über ein Bankkonto verfügen, das direkte Gutschriften zuläßt (durch das US ACH-System). Ebenso wie der Kunde muß er das Registrierungsformular ausfüllen und an FV senden, die eine Registrierungsnummer erstellen. Danach stellt der Anbieter einen Scheck über die Registrierungskosten aus und sendet ihn zusammen mit der Registrierungsnummer und den Bankkonto-Informationen per Post an FV.

Nach erfolgreicher Registrierung können Zahlungstransaktionen ausgeführt werden, die sich bei FV in folgende Schritte unterteilen:

- Der Kunde sendet dem Anbieter per E-Mail seine VirtualPIN und bittet um Zusendung des gewünschten Produktes. Dieser kann die VirtualPIN ohne großen Aufwand als gültig verifizieren.
- Der Anbieter sendet dem Kunden das angeforderte Produkt per E-Mail oder Post zu.
- Ebenso wird vom Anbieter an First Virtual die Kunden-VirtualPIN zusammen mit dem Zahlungsbetrag übermittelt.

- Der Kunde kann nun das Produkt testen.
- Nach angemessener Zeit sendet der FV-Zahlungs-Server dem Kunden eine E-Mail, in welcher dieser den Kauf bestätigen und somit die Zahlung veranlassen soll. Der Anbieter erhält eine Kopie der Kundenreaktion.
- Falls der Kunde mit „Ja“ bestätigt, wird der Betrag noch am selben Tag dem Kunden belastet und dem Anbieter abzüglich der FV-Gebühren gutgeschrieben.
- Bei einem „Nein“ des Kunden wird die Zahlung nicht ausgeführt. Falls dies jedoch häufig geschieht, wird die VirtualPIN des Kunden gelöscht.
- Es besteht auch die Möglichkeit mit „Fraud“ zu antworten, wenn der Kunde beispielsweise der Ansicht ist, daß seine VirtualPIN mißbräuchlich verwendet wird. FV löscht auch in diesem Fall die VirtualPIN.

Das System unterstützt mehrere Sprachen und, bedingt durch die Kreditkarten-Basiertheit, auch mehrere Währungen. First Virtual ist das einzige System, daß dem Kunden erlaubt, das Produkt vor dem Kauf zu testen.

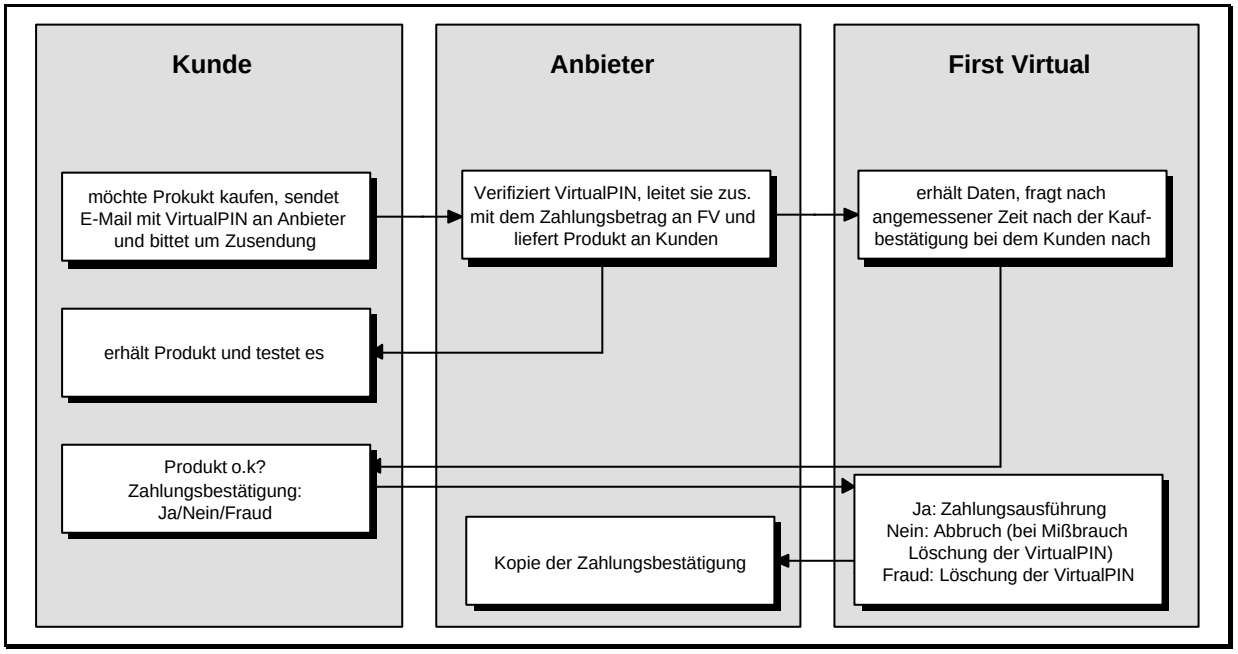

Abbildung 4.11: Zahlungstransaktionsprozeß bei First Virtual

Obwohl First Virtual keine Verschlüsselung bei Zahlungstransaktionen vornimmt, wird das System intensiv genutzt. Eventuell ist das auf den Ablauf der Transaktion zurückzuführen und die damit verbundene Produktauslieferung vor der Zahlung.

[18] URL: http://www.fv.com/newacct/index.html

4.3 CyberCash

Name des Zahlungssystems	CyberCash (Firma CyberCash wurde im August 1994 von William Melton und Daniel Lynch gegründet)
Entwickler	William Melton, Daniel Lynch, u.a.
Prototyp/Test seit	März 1995
Einführung am	April 1995
Grundcharakteristik	Systembeschreibung laut [Wayner96, 131-143]: • Kreditkartensystem, das mit Web-Browser zu bedienen ist • RSA- (768-bit; Ende 1996:1024-bit) und DES- (56-bit) Verschlüsselung, kreiert digitale Signaturen • Kunden-Software läuft auf MS Windows und Macintosh; eine UNIX-Version ist geplant • Anbieter-Software ist für die Plattformen Solaris, BSDI, Sun OS, Windows NT, SGI Irix, HP UX, und Linux vorhanden • funktioniert durch Firewalls • Kommunikation zwischen Anbieter, Kunde und dem CyberCash-Server basiert auf HTTP • Kommunikation zwischen dem CyberCash Gateway und den Kreditkarteninstituten basiert auf dem vorhandenen Finanznetzwerk • Kreditkarten-Transaktionen sind ähnlich wie iKP Struktur • CyberCash ist ein Mittler zwischen dem Verkäufer und der Bank und leistet die Verschlüsselungsarbeit • keine Zertifizierungsstruktur vorhanden • Schlüsselerstellung von CyberCash • US Kreditkartengesellschaften haften für Schaden über US$50, was die Kundenakzeptanz erhöht • Kunde-zu-Kunde Transaktionen sind geplant • keine Sicherheitsschwächen bekannt (keine Anonymität)
praktischer Einsatz/ Marktreife	• CyberCash hat im Mai 1995 die Exportbewilligung erhalten[19]. • Es nehmen achtzehn Banken teil (Stand August 1996), davon sind zehn direkt über das Internet erreichbar. • Weitere Teilnehmer aus dem Finanzsektor sind sechs Finanzdienstleistungs-Agenten (Stand August 1996). • Es bestehen stategische Verbindungen mit Cisco Systems, Intel Corporation und VeriFone. • Mit VISA, MasterCard und American Express definieren sie Protokolle und implementieren SET. • Mit SLIGOS (Zahlungssystem-Anbieter in Europa) plant CyberCash die Einführung in Europa[20]. • Mit Point Scandinavia AS (Provider elektronischer Transaktions-Services) ist die Einführung von sicheren Electronic Commerce Systemen in Schweden geplant[21]. • Es besteht eine Zusammenarbeit mit DEC[22]. • Anfang Juni 1996 hat NetConsult Communications aus Jena seine INTERSHOP Online Software angekündigt, die vollständig mit Ja-

[19] vgl. http://www.CyberCash.com/CyberCash/news/news.html
[20] vgl. http://www.CyberCash.com/CyberCash/news/releases/96mar18a.html
[21] vgl. http://www.CyberCash.com/CyberCash/news/releases/96mar18.html
[22] vgl. http://www.CyberCash.com/CyberCash/news/releases/96mar25.html

	va entwickelt wurde und CyberCash als Zahlungssystem implementiert hat[23]. • American Online (AOL) hat eine CyberCash-Lizenz für ihre Electronic Commerce Strategie im Mai 1996 erworben. Mit dieser Verbindung will AOL (RSA, Terisa Systems, IBM InfoMarket und VeriSign sind ebenso involviert) eine Architektur für sicheren Electronic Commerce bereitstellen[24]. • Anfang Juni 1996 kündigten CyberCash und die National Bank of Canada eine Partnerschaft an. Kunden dieser Bank werden CyberCash innerhalb kurzer Zeit zur Nutzung zur Verfügung haben[25]. • Elektronische Schecks werden voraussichtlich Anfang 1997 und elektronische Münzen gegen Ende 1996 verfügbar sein[26]. • Xerox verkauft seit Ende Juni 1996 Services von seiner „Business Research Group“ in Form von Untersuchungsberichten, die mit dem CyberCash-Wallet bezahlt werden können[27].
Probleme	• geschlossenes System • keine Rückerstattungen • keine Stornierung ausgeführter Zahlungen
URL	http://www.CyberCash.com/

Tabelle 6: CyberCash-Fakten

Die Kundenregistrierung bei CyberCash ist einfach gestaltet, Voraussetzung ist eine gültige Kreditkarte. Der Kunde kann sich auf einer CyberCash Web-Seite[28] das CyberCash-Wallet herunterladen und mit seinen Kreditkartennummern und seinen eigenen Präferenzen bestücken.

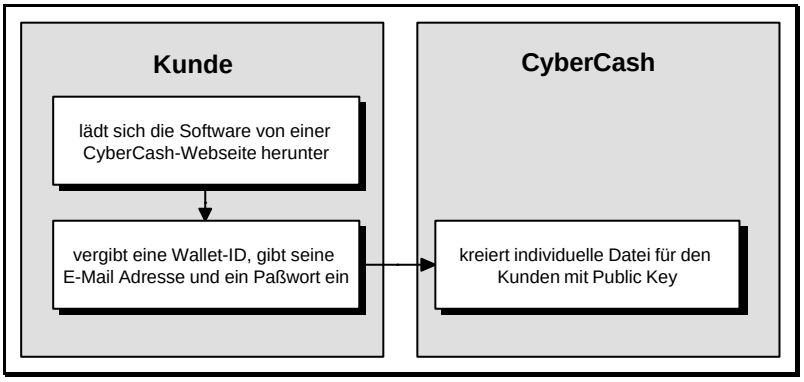

Abbildung 4.12: Kunden-Registrierungsprozeß bei CyberCash

Mit der Installierung der Software erfolgt auch die Registrierung des Kunden bei CyberCash, indem eine individuelle Datei mit den Inhalten der Wallet-Identität und des öffentlichen Schlüssels angelegt wird. CyberCash kreiert die Schlüssel für die Teilnehmer selbst.

Die Anbieter-Registrierung ist etwas aufwendiger[29]. Er muß zuerst einen Registrierungsantrag ausfüllen. Nachdem CyberCash diesen erhalten hat, sendet sie dem Anbieter die Software-Lizenz zu, die

[23] siehe *NetConsult Communications announces First Java-Powered Cybershop-in-a-Box/ INTERSHOP Online Company to Offer Virtual Storefront System for 60-Day Free Trial*, Business Wire, 01.06.1996
[24] vgl. http://www.cybercash.com/cybercash/news/releases/96may15.html
[25] vgl. http://www.cybercash.com/cybercash/news/releases/96june5.html
[26] vgl. http://www.cybercash.com/cybercash/news/releases/96june24-1.html
[27] vgl. http://www.cybercash.com/cybercash/news/releases/96june24-2.html
[28] URL: http://ftp.cybercash.com/cgi-bin/download

er wiederum ausfüllen und zurücksenden muß. Nachdem CyberCash dem Anbieter Zugang zur Software („Secure Merchant Payment System“ SMPS) gegeben hat, lädt er diese herunter und installiert sie auf seinem Web-Server. Danach muß er bei seiner Bank nachfragen, ob sie das ACH-Clearing unterstützt. Falls dies nicht der Fall sein sollte, muß er ein Konto bei einer anderen Bank eröffnen[30]. Das Handling für die Einrichtung des Anbieter-Kontos dauert laut CyberCash je nach Bank ein bis zwei Wochen.

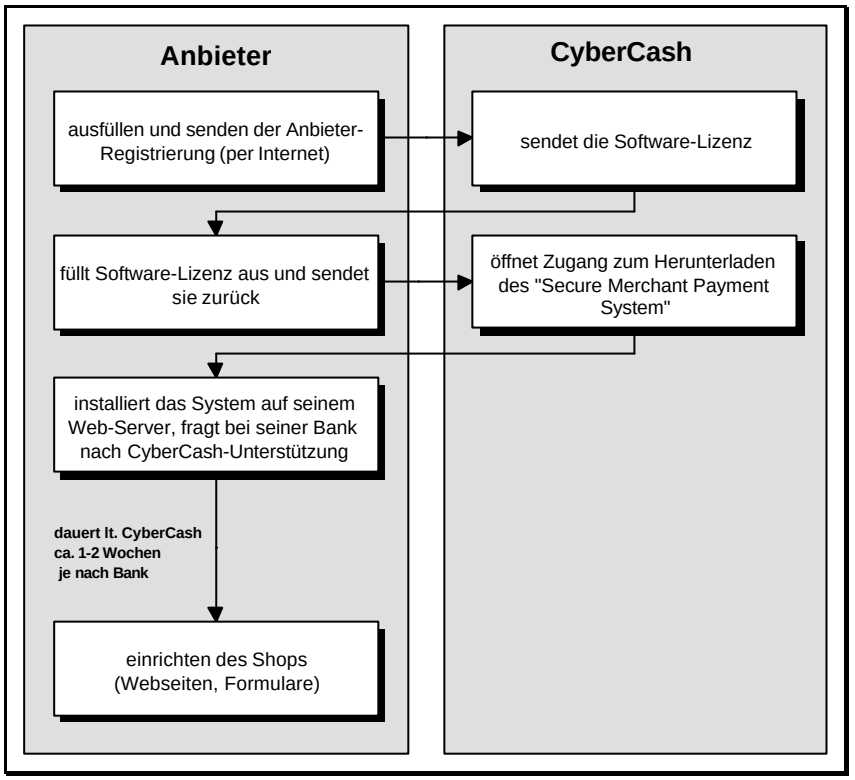

Abbildung 4.13: Anbieter-Registrierungsprozeß bei CyberCash

Die SMPS-Software ist gegen eine geringe Gebühr von CyberCash erhältlich. Wie der Anbieter diese Gebühr begleicht und wie hoch sie ist, ist nicht dokumentiert.

Nachdem der Kunde sein Wallet und der Anbieter seine SMPS-Software erfolgreich installiert und eine zulässige Bankverbindung hat, kann mit dem elektronischen Einkauf begonnen werden.

Die Zahlungstransaktion wird gestartet, sobald der Nachfrager seine gewünschten Produkte ausgewählt und der Verkäufer die Rechnung generiert hat. Durch Nachrichtenversendung (Rechnung) wird beim Kunden lokal das Wallet gestartet. Zukünftig wird den Kunde das Zahlungsmittel in Abhängigkeit der vom Anbieter unterstützten Zahlungsmittel (Kreditkarten, elektronische Schecks oder Münzen) auswählen können. Die Kunden-Software verschlüsselt die sensiblen Daten wie z.B. die Kreditkartennummer und die Transaktionsdaten mit dem öffentlichen Schlüssel des CyberCash-Gateways, unterschreibt die Daten und sendet sie zum Verkäufer. Dieser fügt seine Identifizierungsnummer und nochmals den Rechnungsbetrag hinzu, unterschreibt ebenso, verschlüsselt die Nachricht und sendet sie zum CyberCash Gateway. Dieser authentisiert beide Teilnehmer, entschlüsselt die

[29] vgl. http://www.cybercash.com/cybercash/merchants/getstarted.html

[30] Auf der Page: http://www.cybercash.com/cybercash/financial/bankfin.html sind alle Banken (Anzahl 18) und Finanzdienstleistungs-Agenten aufgelistet, die Konten für Anbieter von CyberCash zur Verfügung stellen.

Rechnungsbeträge, vergleicht sie und sendet die Informationen bei Übereinstimmung und nach Umformatierung zum Kreditkarten-Unternehmen, das die Kreditkarten-Autorisierung vornimmt. Das Resultat wird an das Gateway rückübermittelt und wieder umformatiert. Nachdem der Anbieter die Nachricht von Gateway erhalten hat, wird er das Produkt und eine Bestätigung dem Kunden ausliefern.

Nachfolgend wird nochmals der Ablauf einer Zahlungstransaktion bei CyberCash skizziert:

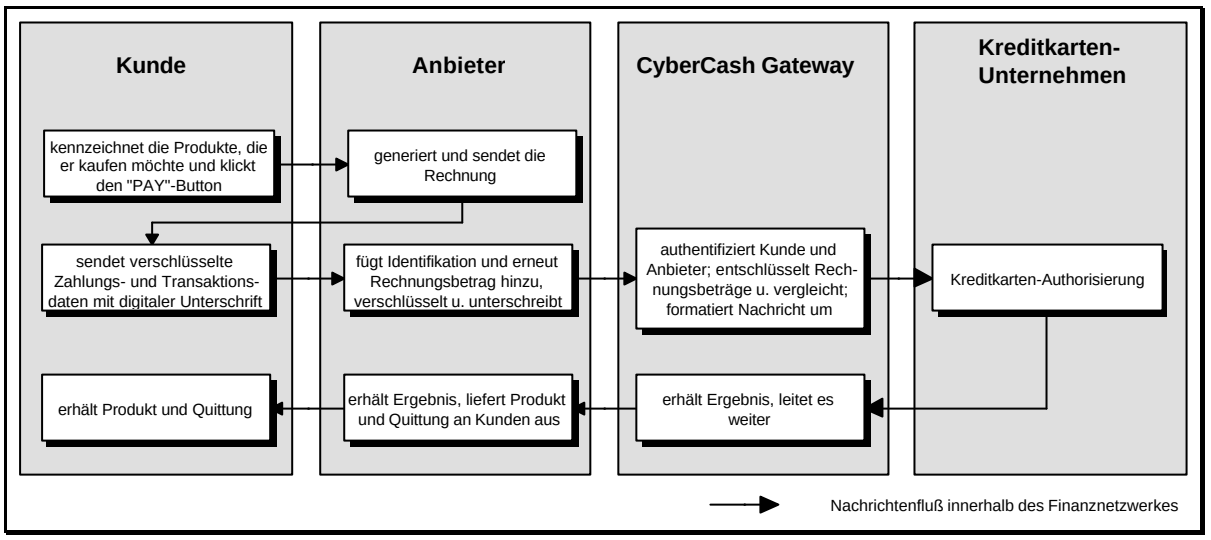

Abbildung 4.14: Zahlungstransaktionsprozeß bei CyberCash

Laut CyberCash sind die Kreditkartennummern ausschließlich beim Kunden gespeichert. Der Anbieter hat keine Möglichkeit, die Nummer zu entschlüsseln und somit kann er sie nicht für seine eigenen Zwecke nutzen. [Wayner96, 133] ist allerdings der Ansicht, das das CyberCash Gateway durchaus in der Lage ist, die Kreditkartennummern der Kunden als Vorteil an die Anbieter weiterzuleiten.

CyberCash wird voraussichtlich auch in der Zukunft eine Rolle spielen. Durch die Einführung von elektronischen Schecks und elektronischen Münzen wird den Marktteilnehmern eine höhere Flexibilität geboten. Weiterhin wird durch die Implementation von SET das Vertrauen in CyberCash steigen und der Marktanteil dadurch angehoben werden.

5 Zahlungssysteme auf Scheck-Basis

5.1 Allgemeines

Bei einem elektronischen Scheck muß laut [Beutelspacher/Hueske/Pfau93, 100] der Scheckaussteller ersichtlich sein, die digitale Signatur muß zweifelsfrei verifiziert werden können, und Zahlungsbetrag und Signatur müssen in eindeutiger Beziehung zueinander stehen. Problematisch ist die mangelnde Aktzeptanz der digitalen Signatur bei den Finanzintermediären in Europa.

Zahlungssysteme auf Scheck-Basis liegen aus Transaktionssicht gesehen näher bei bargeld-ähnlichen Zahlungsmitteln als Kreditkarten, da ein „Kunde-zu-Kunde"-Geldtransfer generell möglich ist. Mit Kreditkarten-Zahlungssystemen haben sie die fehlende Anonymität gemeinsam, da die Zahlungen rückverfolgbar sind [Tanaka96].

Ein möglicher Auslöser für die Durchsetzung von elektronischen Schecks sind die Zahlungsgewohnheiten in den Vereinigten Staaten, wo im Jahre 1988 ca. 50 Milliarden Schecks ausgestellt wurden [Steiner/Teixeira90]. Ob sie sich in Europa durchsetzen werden ist fraglich.

5.2 NetCheque von der University of Southern California

Name des Zahlungssystems	NetCheque
Entwickler	Information Sciences Institute University of Southern California
Prototyp/Test seit	ca. Januar 1995[31]
Einführung am	nicht bekannt
Grundcharakteristik	Mit dem NetCheque Zahlungssystem kann der Benutzer Schecks ausstellen, Geld auf bestimmten Konten deponieren und überweisen. Der elektronische Scheck muß folgende Daten enthalten [Jansen95, 43-44]: • Name des Verkäufers, • Kontonummer des Käufers, • Name des Accounting Servers (AS), • Rechnungsbetrag, • Währung, • elektronische Signatur des Käufers und • das Verfalldatum. Der Benutzer kann mit den o.a. Daten und der *write_cheque*-Funktion von NetCheque einen Scheck generieren[32] und löst ihn anschließend ein. Das Clearingsystem funktioniert wie bei herkömmlichen Schecks über eventuell mehrere Accounting Server (AS-Hierarchie) [Stumpf96, 38]. Wird die Scheckeinreichung per Batchverarbeitung erledigt, so ist die Transaktion gebührenfrei, für die Online-Abwicklung besteht Gebüh-

[31] siehe [Hill95]

[32] siehe http://nii-server.isi.edu/gost-group/products/netcheque/ncgui/wcheque.html

	renpflicht. Der Kunden-AS meldet dem Anbieter, sobald die Zahlung ausgeführt ist, so daß dieser die Lieferung vollziehen kann[33]. Die digitale Signatur wird mit Kerberos, das vom MIT entwickelt wurde, authentifiziert. Es handelt sich um ein verteiltes System, da mehrere AS´s enthalten sind. Eine Kombination mit NetCash ist möglich.
praktischer Einsatz/ Marktreife	kein praktischer Einsatz
Probleme	• keine Anonymität • keine Verbreitung des Systems • keine namenhafte Vertragspartner
URL	http://nii-server.isi.edu/info/NetCheque/

Tabelle 7: NetCheque-Fakten

Die Kundenregistrierung bei dem System NetCheque ist einfach und wird per E-Mail dokumentiert. Die Registrierung beginnt auf der Seite

http://nii.isi.edu/info/netcheque/application.html

wo nach dem Kontonamen, der E-Mail-Adresse, einem Sicherheitsnamen, Sicherheitspaßwort und verschiedenen Optionen gefragt wird.

Nachfolgende Graphik erläutert den einfachen Registrierungsprozeß von Kunden bei NetCheque:

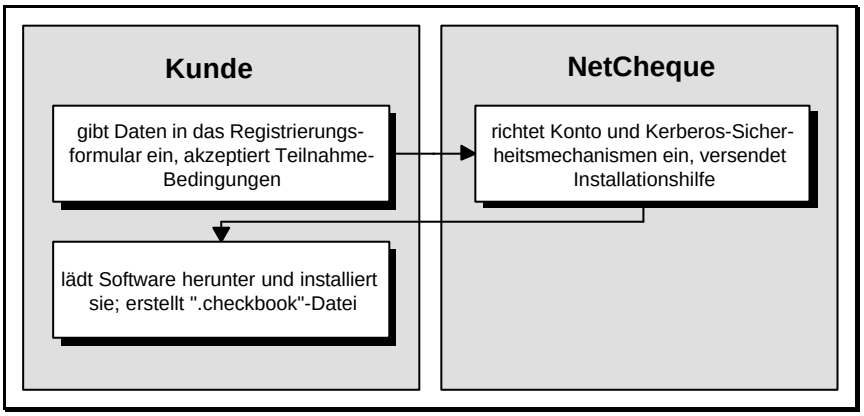

Abbildung 5.15: Kundenregistrierungsprozeß bei NetCheque

Nach versenden dieser Daten über das Internet erhält man postwendend die Kontenbestätigung mit folgenden Anweisungen und Informationen:

- Der Kunde muß die Datei „.checkbook“ im Hauptverzeichnis mit folgendem Inhalt erstellen:

  accsrv_inet_name netcheque.isi.edu
  accsrv_route_name netcheque.isi.edu
  default_currency NCU
  princ_name <Name>/demo@NETCHEQUE.ISI.EDU
  accsrv_krb5_name NetCheque/netcheque.isi.edu@NETCHEQUE.ISI.EDU
  account_id <Vorname_Nachname>

- Installationsanweisung des NetCheque Client-Programms auf dem Rechner

[33] siehe Jansen, Christoph, *Zahlungsprozesse im Internet*, Diplomarbeit an der Univerität St. Gallen, vom 31.08.1995

- Informationen über die individuelle Kerberos-Identifikation mit Paßwort
- Im Anhang befindet sich ein elektronischer Scheck im Wert von 10.000 NCU (Pseudo-Währung), der per „deposit_cheque <Datei>“ bei NetCheque deponiert werden kann.

Die Registrierung für Anbieter ist auf folgender WWW-Seite erläutert:

http://nii.isi.edu/info/netcheque/license.html

Der Zahlungsprozeß von NetCheque läuft folgendermaßen ab: Im ersten Schritt erstellt der Kunde mit der *write-cheque*-Funktion seiner Client-Software einen elektronischen Scheck, der mit Kryptomechanismen gesichert und zum Anbieter weitergeleitet wird. Dieser leitet den Scheck mit der *deposit-cheque*-Funktion in das AS-Netzwerk weiter, in welchem die Überprüfung und Scheckeinlösung stattfindet. Sowohl Kunde als auch Anbieter erhalten vom AS eine Benachrichtigung, wenn der Scheck weitergeleitet oder eingelöst wird. Nach der Scheckeinlösung erfüllt der Anbieter seine Lieferungspflicht.

Einen zusammenfassenden Überblick über den Zahlungsrozeß bei NetCheque gibt nochmal die untenstehende Graphik:

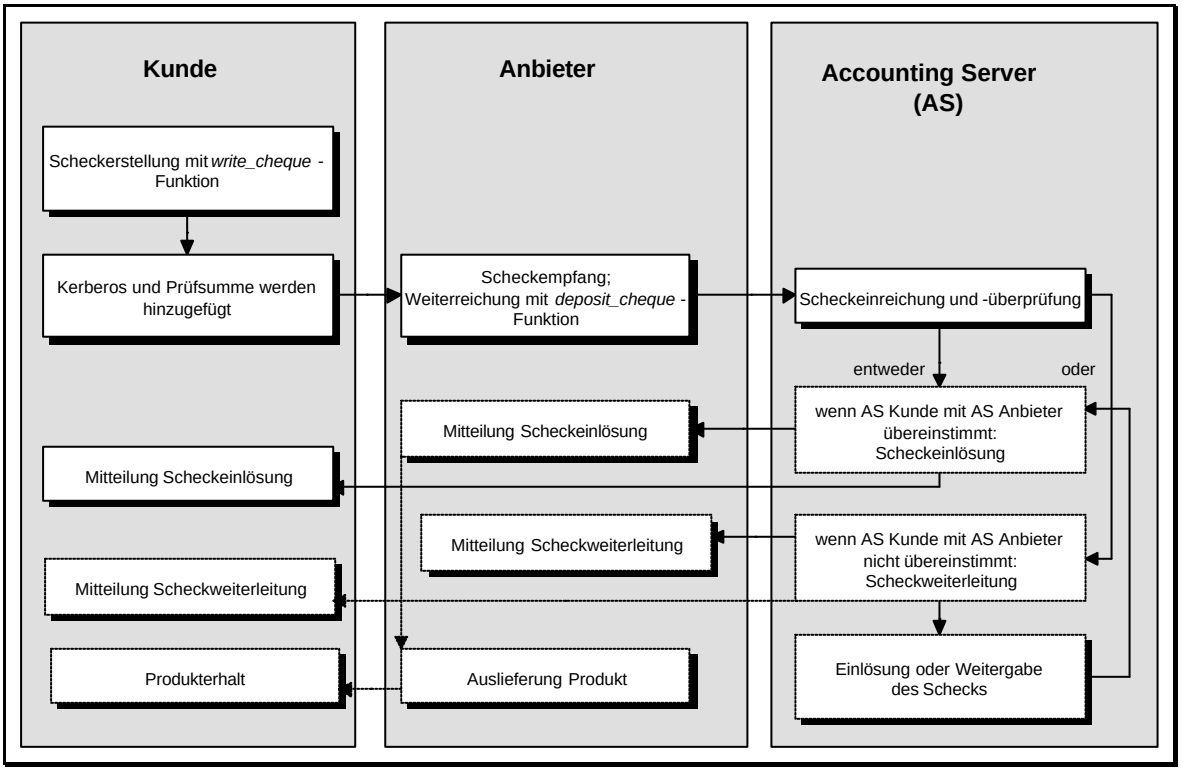

Abbildung 5.16: Zahlungstransaktionsprozeß bei NetCheque

In Anbetracht der Tatsache, daß ein kommerzieller Einsatz von NetCheque noch nicht stattgefunden hat, sind Aussagen über das Entwicklungspotential dieses Systems recht schwierig.

5.3 Weitere Zahlungssysteme auf Scheck-Basis

Nachfolgende Tabelle gibt einen Überblick über weitere elektronische Zahlungssysteme auf Scheck-Basis und deren Fundstelle im Internet:

Redi-Check	URL: http://websites.earthlink.net/~shurie/redi/
NetChex	URL: http://www.netchex.com
Checkfree	URL: http://www.checkfree.com
FSTC Electronic Check Project	URL: http://www.llnl.gov/fstc/projects/checking.shtml

Tabelle 8: Weitere elektronische Scheck-Systeme

6 Zahlungssysteme auf SmartCard-Basis

6.1 Allgemeines

Im Gegensatz zu den anderen bereits erwähnten Zahlungssystemen, die überwiegend in den USA entwickelt und genutzt werden, stellt sich die Entwicklung von Chipkarten bzw. SmartCards (auch als „stored value card“ bezeichnet) besonders in Europa in den Vordergrund [Foremski96] [Anderer95].

SmartCards besitzen einen Chip bzw. bestehen als Übergangslösung aus einem Magnetstreifen zuzüglich Chip. Sie bieten beim Zahlungsverkehr durch ihre integrierten Verschlüsselungsmechanismen hohe Sicherheit. Ebenso zeichnet sich die multifunktionale SmartCard, die beispielsweise auch als Kreditkarte und Sozialversicherungsausweis dienen kann, durch Komfort und Anwenderfreundlichkeit aus[34].

Ein Nachteil der SmartCard-Lösung ist der verhältnismäßig teure Kartenleser, der am Client-Rechner zu installieren ist [Anderer95]. Jedoch kann aufgrund des Chips, der die Kryptographieschlüssel gespeichert hat, eine Transaktion auf hohem Sicherheitsniveau stattfinden [Martin96].

Die enorme Entwicklung und Verbreitung der SmartCards spiegeln sich auch in den stattfindenden Pilotprojekten wider, welche die Zukunftsaussichten für dieses Zahlungsmittel erhöhen.

SmartCards im Internet/Netzwerken nach [Block/Kingson Bloom/Kutler96]:

⇒ VISA International startete im Juli 1996 einen Pilot mit zwei großen Pariser Banken, der den Electronic Commerce durch Heimcomputer mit integrierten Chipkartenlesern demonstrieren soll.

⇒ WebTV Networks Inc. in New York entwarf im Juli 1996 eine „Television Set-Top-Box“ mit SmartCard-Leser, der u.a. für das Internet und Online-Banking verwendet werden kann.

[34] siehe o. V. *Chipkarte - griffiges Medium*, IBM Nachrichten, Nr. 44, 1994, S. 66-68

⇒ Im Juni 1996 bei der Europay International Tagung in Spanien initierte die International Business Machines Corp. Cash-Transfers mit SmartCards (PC und Kartenleser).

Kommerzielle SmartCard-Produkte (nicht im Internet):

⇒ portugiesisches Geldbörsensystem SIBS von PMB (Porta Moedas Multibanco) [Klein95]
⇒ östereichisches Geldbörsensystem QUICK [Klein95]
⇒ Geldbörsensystem des ZKA [Klein95]
⇒ belgisches Geldbörsensystem PROTON [Bergdolt96]
⇒ und viele mehr

Verschiedene Pilotprojekte mit SmartCards:

⇒ In Afrika (Zambia) findet derzeit ein Pilot von SmartCards mit der Barclays Bank (England) statt [Foremski96].
⇒ Im Ravensburger Pilotprojekt[35] sind 80.000 Chipkarten an Kunden und 1.000 Händlerterminals verteilt worden [Bergdolt96].
⇒ VISA und MasterCard führen mit zwei New Yorker Banken seit Anfang April ein Pilotprojekt durch[36].
⇒ Ein weiteres Pilotprojekt von VISA fand in Atlanta bei den olympischen Spielen statt[37].
⇒ Die landesweite Einführung von VISA Cash wird im Laufe von 1996 in Spanien stattfinden[38].
⇒ China plant bis zum Jahr 2000 die Ausgabe von 300 Millionen SmartCards (Golden Cards) [Foremski96].

Bisher werden SmartCards kaum über das Internet genutzt. Aufgrund ihrer kommerziellen Verbreitung, der hohen Sicherheitsaspekte und der günstigen Abwicklungsmöglichkeiten aufgrund ihrer Offline-Fähigkeit bieten SmartCards eine hervorragende Zahlungsmöglichkeit im Internet, besonders in Bezug auf Micropayments.

Nachfolgend wird auf zwei SmartCards eingegangen. Beide Systeme sind noch nicht über das Internet für Zahlungen nutzbar.

6.2 Mondex von Jones und Higgins

Name des Zahlungssystems	Mondex
Entwickler	Tim Jones und Graham Higgins (NetWest Bank, England)
Projektvorhaben seit	März 1990
Prototyp/Test seit	März 1992: „Byte"-Versuch im NatWest-Hauptgebäude in London; 6.000 Testpersonen Juli 1995 - Juli 1997: Feldversuch in Swindon, Südengland
Einführung am	bisher keine Nutzung im Internet
Grundcharakteristik	Mondex ist ein offline Kartenzahlungssystem, das auf der SmartCard-

[35] vgl. auch o. V. *Ravensburger Spiele - ein Kommentar*, Karten, Feburar 1996; und [Sperlich96]
[36] siehe InfoWorld *Internet could see cash transfers soon*, 16.04.1996
[37] siehe o. V. *Going for Olympic gold cards*, The Economist, March 30th 1996, S. 73 - 74
[38] siehe o. V. *Elektronische Geldbörse in Spanien*, Karten, Februar 1996

	Technologie basiert und an ein Bankkonto gebunden ist. Aufladen und Bezahlen kann man mit Hilfe eines Kartenlesers per Telefon oder über Computernetze; es sind auch Geldtransfers auf andere Mondex-Karten möglich. Das System wird im „alltäglichen Leben“ verwendet, z.B. zum Fahrscheinlösen in Bussen. Insgesamt können fünf verschiedene Währungen gespeichert werden. Jeder Geldschein ist elektronisch unterschrieben. Die Hardware ist als manipulationssicher bekannt [Janson/Waidner96a]. Durch die stetige Weitergabe der Geldscheine ist ein hohes Anonymitätslevel gewährleistet, obwohl für die Weitergabe an sich keine Verschlüsselungsmechanismen angewandt werden, nur zur Identifizierung generiert die Karte digitale Signaturen. Finanziert wird Mondex, indem die teilnehmenden Banken eine Lizenz kaufen müssen [Bergdolt96]. Weiterhin bezahlen die Kunden Kartengebühren von 1,50 Pfund im Monat, wobei die ersten sechs Monate gebührenfrei sind [Fischer95]. Es sind keine Transaktionskosten zu bezahlen.
praktischer Einsatz/ Marktreife	Seit 1992 ist die englische Telefongesellschaft British Telecom für die technische Seite des Systems zuständig. 1993 wurde die Midland Bank ebenso Teilnehmer an Mondex. Im Oktober 1994 kaufte die Bank of Honkong Mondex für den Fernost. Im Juli 1995 hat die Wells Fargo Bank ein Mondex-Projekt mit einigen ihren Mitarbeitern gestartet. Im Mai 1995 verpflichteten sich die Royal Bank of Canada und die Canadian Imperial Bank of Commerce dazu, Mondex in Kanada einzuführen; für 1996 ist ein Pilotprojekt geplant und in 1997 die Produktion und der Einsatz der Mondex-Systeme. Ende Mai 1996 wurde eine Vereinbarung veröffentlicht, die beinhaltet, daß VeriFone (Provider für sichere Zahlungssysteme) ermöglicht wird, Hardware und Software anzubieten, die Kompatibilität zu Mondex aufweist[39]. Zudem beabsichtigt Tim Jones Mondex in Japan einzuführen, wo sie bereits mit der Industrial Bank of Japan und anderen Banken Übereinkünfte geschlossen haben[40] und auch mit dem Wallet-Hersteller Matsushita Group ein gemeinsames Projekt starten wollen[41]. Seit dem 18. Juni 1996 wird Mondex von zehn führenden Banken in Australien und Neuseeland angeboten[42]. Mondex verfolgt das Ziel, weltweit Marktführer von Kartengeld zu werden [Bergdolt96]. In Deutschland sind bereits einige Interessenten mit der National Westminster Bank im Gespräch [Sperlich96].
Probleme	noch nicht über das Internet verfügbar
URL	http://www.mondex.com/index.html

Tabelle 9: Mondex-Fakten

Anhand des CEN-Standards, der sieben Teilnehmer-Rollen für eine branchenübergreifende elektronische Geldbörse definiert [Klein95] wird unten aufgeführte Graphik mit ihren Teilnehmern erläutert:

[39] siehe *Mondex expected to gain worldwide compability with VeriFone Systems*, Press Release Newswire, 20.05.1996

[40] siehe *Mondex electronic cash system available soon in Japan*, Nikkei English News, 20.05.1996

[41] siehe *Matsushita to invest in electronic cash venture with Mondex U.K.*, Nikkei English News, 20.05.1996

[42] siehe *Ten Leading Banks in Australie and New Zealand Put Their Money on Mondex*, http://www.mondex.com/mondex/austnz.htm

⇒ Der National Originator übernimmt die Aufgabe des Geldbörsenherausgebers (Purse Provider); er ermöglicht das Aufladen der SmartCards und sammelt das Geld von den Händlerbanken wieder ein.

⇒ Die Kundenbank dient als Schnittstelle zwischen dem Kartenhalter und dem Geldpool; sie stellt den Ladebeauftragten (Load Agent) dar. Über sie kann der Kartenhalter per Geldautomat und Telefon (zukünftig auch per Internet) einen Wertetransfer vornehmen.

⇒ Der Kartenhalter (Purse Holder) besitzt die Mondex-Karte und kann Einkäufe damit tätigen und das Geld an andere Konsumenten übertragen.

⇒ Der Service Provider stellt den Einzelhändler dar.

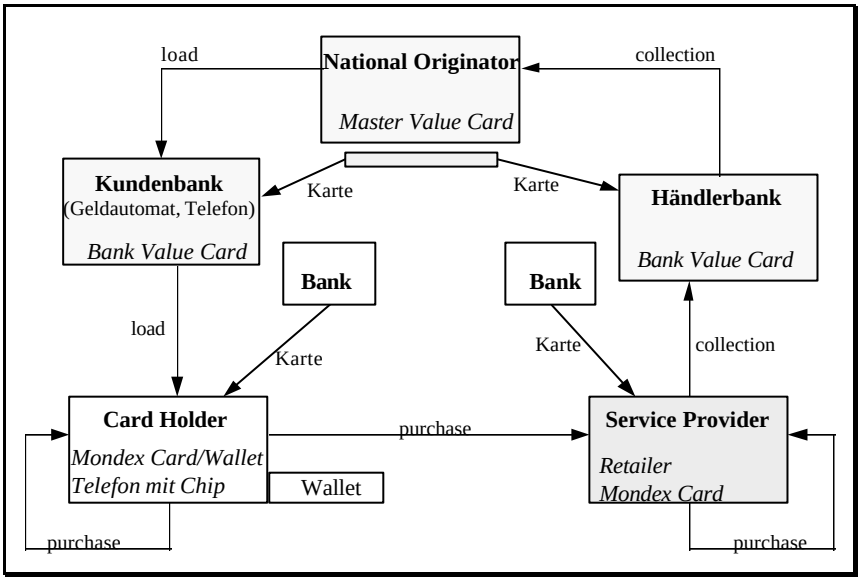

Abbildung 6.17: Das Mondex-System [Klein95]

Aus der Graphik ist der geschlossene Kreislauf von SmartCard-Systemen zu sehen, abgehobenes Geld wird nach einem bestimmten Zeitraum wieder zur ausgebenden Stelle zurücktransferriert. Detailliertere Informationen über das Mondex-System und SmartCards allgemein sind [Klein95] und den Mondex-Magazinen[43] zu entnehmen.

Mondex möchte in absehbarer Zeit auch online-Einkäufe Internet ermöglichen. Zum Zeitpunkt der Erstellung der vorliegenden Arbeit wurde das System jedoch noch nicht über das Internet genutzt[44].

6.3 CAFE

Name des Zahlungssystems	CAFE
Entwickler	Projekt des ESPRIT-Programms der EU
Projekt	Oktober 1992 bis ursprünglich November 1995; Verlängerung des Feldversuchs bis Ende Februar 1996

[43] Mondex-Magazine können auf der WWW-Page http://www.mondex.com/newslet.htm eingesehen werden.
[44] lt. E-Mail von Brita Latham am 09.08.1996

Prototyp/Test seit	Oktober 1995 im EU-Kommissionsgelände in Brüssel (nicht im Internet)
Einführung am	keine Einführung im Internet geplant
Grundcharakteristik	CAFE ist ein elektronisches Zahlungssystem, bei dessen Entwicklung schwerpunktmäßig auf die Sicherheit der Teilnehmer eingegangen wurde. Das System wurde in zwei Varianten entwickelt. Die erste ist eine SmartCard, die Geld speichert und mit Hilfe eines Kartenlesers Geldtransfers durchführen kann. Mit Hilfe von Infrarotstrahlen wird die Verbindung von Terminal zum Kartenleser hergestellt. Der Kartenleser enthält lediglich zwei Buttons, den „On"- und den „Pay"-Button. Die zweite Variante ist eine elektronische Geldbörse, deren Transaktionen mit einer PIN beginnen. Für die Verbindung wird ebenfalls Infrarot verwendet. Durch RSA-Verschlüsselung wird die Privatsphäre des Benutzers geschützt, auf Wunsch kann die Identifizierung gewählt werden. Dreizehn Partner von verschiedenen Ländern nahmen an diesem Projekt teil, u.a. Digicash, die Universität Hildesheim, die Universität Freiburg und SIEMENS. Fünf verschiedene Währungen können auf der SmartCard gespeichert werden. Bei Kartenverlust kann der Restbetrag ermittelt und somit erstattet werden. Die offene Architektur ermöglicht die Teilnahme mehrerer Banken, Händler und Kunden.
praktischer Einsatz/ Marktreife	Von Oktober 1995 bis Ende Februar 1996 wurde CAFE im EU-Kommissionsgelände getestet. Die Ergebnisse zeigten, daß ein solches System machbar ist. Das Bezahlen dauerte bei 7 Mhz 1,2 bis 1,5 Sekunden[45]. CAFE wird innerhalb des OPERA-Projekts weitergeführt.
Probleme	CAFE wurde als Forschungsprojekt durchgeführt, die kommerzielle Nutzung war nicht geplant.
URL	http://www.informatik.uni-hildesheim.de/~sirene/projects/cafe/ index.html und http://www.digicash.com/products/projects/cafe.html

Tabelle 10: CAFE-Fakten

Anfang des Jahres 1996 haben Banken aus Griechenland das Konsortium OPERA (Open Payments Research Association) gegründet, um den Versuch in Brüssel fortzuführen. Das Projekt wird voraussichtlich im zweiten Quartal 1997 beendet sein, eventuell wird es ausgedehnt. Der Fokus liegt auf fortgeschrittener Kryptographietechnik in Zahlungskarten. Eines der Ziele ist der Test von Kundenkarten, die Kredit, Debit und „Bargeld" auf *einem* Chip beinhaltet. Weiterhin wollen die Banken neue Pilote in Süd-Europa starten[46].

7 Zahlungssystem auf EDI-Basis

7.1 Allgemeines

[45] lt. Arnd Weber, E-Mail vom 18.04.96

[46] Die Informationen sind einem Telefax von Chris Standford, CardWare Ltd., England, entnommen. CardWare Ltd. ist für die Administration des OPERA-Projekts zuständig.

Unter Electronic Data Interchange (EDI) versteht [Mausberg95, 64ff.] den elektronischen Austausch von Daten, Texten oder Multimedia-Komponenten zwischen Rechnern unterschiedlicher Unternehmungen in einem standardisierten Format. Dabei muß die Syntax und die Semantik der auszutauschenden Information festgelegt sein. Ziel von EDI ist die Ablösung der papiergebundenen Geschäftsabläufe und die Verhinderung von Medienbrüchen. Der Informationsfluß und die Informationsverwaltung wird verbessert [Mausberg95, 64]. Denn durch die elektonische Übermittlung wird die Datenerfassung minimiert bzw. entfällt und Erfassungsfehler reduzieren sich [Oesterle93]. Standards für EDI-Nachrichten sind Edifact und UN/Edifact. Detaillierte Beschreibungen von EDI und Edifact sind in [Krähn93, 30ff] und [Hitachi93, 93ff.] zu finden. [Lindemann96] erläutert detailliert die E-Mail-basierte Nachrichtenübermittlung im Internet.

Da EDI im Internet eine wesentlich günstigere Alternative (aufgrund dem *store-and-forward*-Mechanismus und der Tatsache des Internets als „preisgünstige Kommunikationsplattform“) ist [Klein/Lindemann96] [Cameron96, 232], wird die Einstiegsbarriere für EDI verringert.

Nachdem EDI früher nur in VAN’s benutzt wurde, wird heute das Internet als weitere Kommunikations-Infrastruktur untersucht und Pilotversuche unternommen, z.B. Wells Fargo [Cameron96, 232] und NACHA[47]. Daß die Ausrichtung von EDI und dessen Standards auf den kommerziellen Bereich die Integration des *Privatkunden* nicht behindert, zeigt sich am Beispiel des TeleCounters.

7.2 TeleCounter

Name des Zahlungssystems	TeleCounter
Entwickler	Kompetenzzentrum TeleCounter des Instituts für Wirtschaftsinformatik an der Universität St. Gallen
Prototyp/Test seit	Januar - Juni 1994 über das Internet
Einführung am	noch keine kommerzielle Nutzung
Grundcharakteristik	Der TeleCounter ist ein Zahlungsverkehrskonzept, das mit Edifact-Nachrichten den klassischen Überweisungsverkehr (Rechnungs-Überweisungen, Gutschriften und Belastungen) abbildet und das sich in den Gesamtkontext eines elektronischen Marktes einordnen läßt [Mausberg95, 106]. Mit der TeleCounter Client-Software kann der Kunde Zahlungsaufträge ausführen, die durch eine Rechnung induziert worden sind. Der Client generiert die Edifact-Nachrichten bzw. empfängt und liest sie hinterher. Beteiligte sind Finanzdienstleister, welche die Edifact-Nachrichten entgegennehmen. Dazu verwenden sie entweder einen „Vorrechner“, der die Nachrichten überprüft, oder einen Edifact-Server, der die Daten via EDI-Gateway an das Bankensystem weiterleitet. Kommunikationsmittler, die den Finanzdienstleistern vorgeschaltet sind, übernehmen die Konvertierung der Daten und leiten sie weiter. Auch andere Edifact-Finanzmeldungen, wie sie in [Mausberg95, 80] erläutert werden, sind möglich. Alle Transaktionen des TeleCounters bilden einen geschlossenen elektronischen Kreislauf ab. Hard- und Software-Voraussetzungen für Kunden sind ebenso in

[47] siehe Projekt *Bankers Electronic Data Interchange (EDI) Council*, http://www.nacha.org/bedic.htm

	[Mausberg95, 123] ausführlich erläutert. Für Micropayments ist dieses Zahlungssystem nicht geeignet.
praktischer Einsatz/ Marktreife	noch kein praktischer Einsatz
Probleme	Die Banken wollen EDI nicht im Retailbereich nutzen.
URL	http://www-iwi.unisg.ch/iwi4/cc/tc/

Tabelle 11: TeleCounter-Fakten

Aus dem TeleCounter-Pilot ergaben sich folgende Nutzen für den Finanzdienstleister. Wie auch bei anderen elektronischen Zahlungssystemen vermindert sich der Aufwand der bankinternen Erfassung im Vergleich zum papiergebundenen Zahlungsverkehr. Weiterhin fallen keine Wartungen und Systempflege für Applikationen an, da alle Banken das Edifact-Format verarbeiten können und die Infrastruktur somit vorhanden ist. Durch die Einführung eines Edifact-Servers könnte eine Bank die Schnittstelle für alle Kunden (Großkunde, KMU und Retailbereich) vereinheitlichen.

Durch die Multibankfähigkeit des TeleCounters wird dem Kunden die gemeinsame Verwaltung von Konten verschiedener Kreditinstitute ermöglicht. Von der intelligenten Client-Software wird die Kennung des betreffenden Kreditinstitutes in der zu versendenden Nachricht übernommen. Der Kommunikationsmittler leitet den Zahlungsauftrag direkt an die von der Client-Software gekennzeichnete Bank; dem Kunden wird somit ein hohes Maß an Komfort geboten.

Nachfolgende Graphik verdeutlicht den Ablauf einer Zahlungstransaktion mit dem TeleCounter:

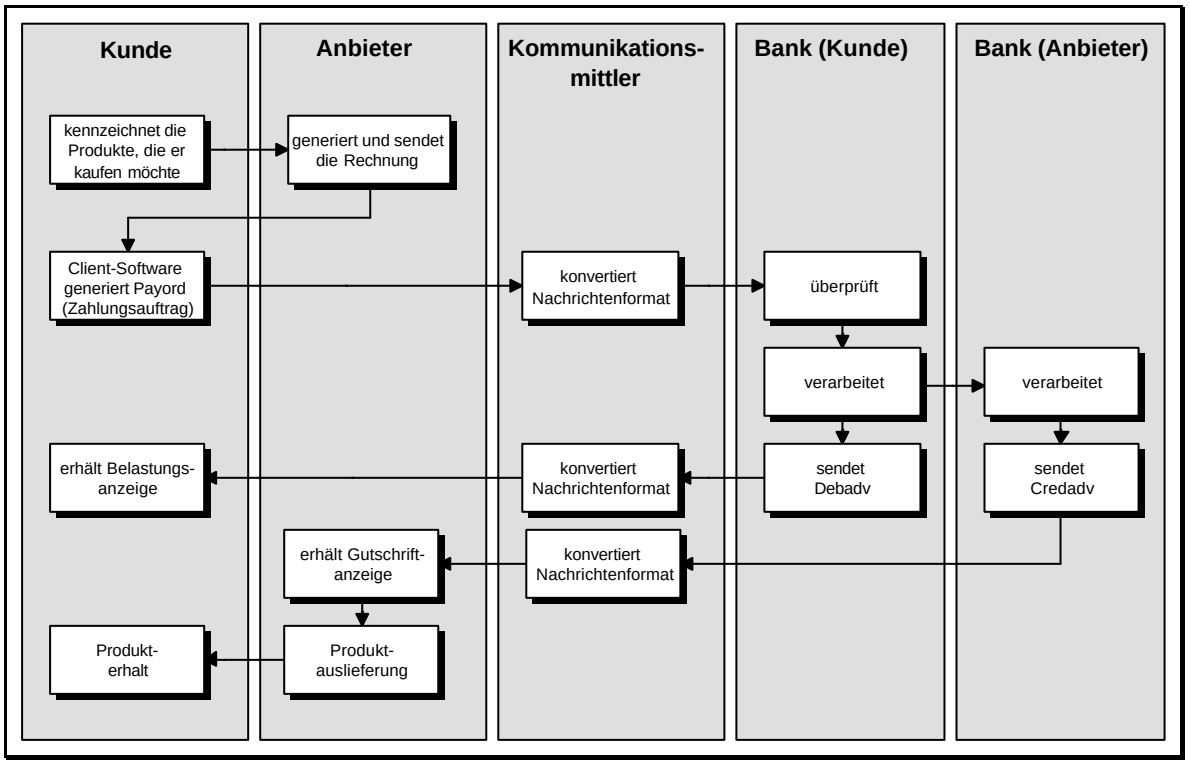

Abbildung 7.18: Zahlungsprozeß mit dem TeleCounter

Der TeleCounter Pilot hat bewiesen, daß mit einer geeigneten Client-Software EDI auch im Retailgeschäft erfolgreich einsetzbar ist. Den beteiligten Banken wurde bei dem Pilotprojekt sehr stark die

Offenheit bewußt, die das Internet mit sich bringt. Trotz der Tatsache, daß die Abwicklung von Transaktionen nach dem TeleCounter-Konzept funktioniert und die Banken einen großen Nutzen aus dem System ziehen können (keine Neuerfassung, vorhandene Infrastruktur), möchten sie die Nutzung von EDI bisher auf den Geschäftsbereich beschränken.

Das TeleCounter-Konzept basiert auf dem Austausch standardisierter Nachrichtenformate mit dem Zweck der Abwicklung von Bankgeschäften, insbesondere dem Zahlungsverkehr. Somit stellt das Konzept eine typische Telebanking-Lösung dar, wie von [Straub90, 132] definiert wurde:

> Telebanking umfaßt alle Möglichkeiten und Techniken, die dem Kunden ermöglichen, von seinem Standort aus, unter Benützung telematischer Systeme, direkt Bankgeschäfte zu erledigen.

Diese Definition stammt aus einer Zeit, als Videotex das einzige interaktive Telematikmedium für das Retailsegment war und elektronische Zahlungssysteme im Internet nicht oder nur kaum diskutiert wurden.

8 Bewertung der Zahlungssysteme

Zusammenfassend werden in diesem Kapitel einige vorgestellte Zahlungssysteme anhand der aufgestellten Bewertungskriterien beurteilt (Stand: August 1996).

Technische Kriterien (Stand Oktober 1996)	Ecash	Net-Cash	First Virtual	Cyber-Cash	Net-Cheque	Mon-dex	CAFE	Tele-Counter
Eingesetzte Verschlüsselungs-verfahren								
Symmetrische Verfahren	nein	ja	nein	ja	ja	ja	nein	ja
Asymmetrische Verfahren	ja	ja	nein	ja	nein	ja	ja	nein
Hash-Algorithmen	ja	nein	nein	ja	nein	ja	nein	nein
Sicherheitsmechanismen								
Digitale Signatur	ja	ja	nein	ja	ja	ja	ja	nein
Zertifizierung	nein	ja[48]	nein	nein	ja[49]	nein	nein	nein
Sicherheitsanforderungen								
Vertraulichkeit	ja	ja	nein	ja	ja	ja	ja	ja
Integrität	ja	ja	nein	ja	ja	ja	ja	ja
Authentifizierung	ja	ja	ja	ja	ja	ja	ja	ja
Autorisierung	ja	ja	ja	ja	ja	ja	ja	ja
Non-Repudiation	nein	nein	nein	nein	nein	nein	nein	nein
Vermeidung von Attacken	ja	ja	nein	ja	ja	ja	ja	ja
Realisierung und Integration								
Zahlungskommunikation (online - offline)	beides	beides	offline	online	beides	offline	offline	offline
Durchgängigkeit der IT-Mittel[50]	nein[51]	ja	nein	ja	ja	ja	ja	ja

[48] Der Währungsserver benutzt Public-Key-Zertifikate für die eigene Identifizierung, die ihn ermächtigt, den anderen Teilnehmern Münzen auszugeben. Der Benutzer besitzt jedoch kein Zertifikat. [Wayner96 82].

[49] NetCheque benutzt keine Public-Key-Zertifikate, jedoch hat die Verschlüsselung mit Kerberos den gleichen Effekt [Wayner96 82].

[50] Die erste Einzahlung auf das bei dem Systemanbieter/Finanzinstitut eröffnete Konto wurde hierbei nicht berücksichtigt.

Technische Kriterien (Stand Oktober 1996)	Ecash	Net-Cash	First Virtual	Cyber-Cash	Net-Cheque	Mon-dex	CAFE	Tele-Counter
Integrationsfähigkeit (Marktplattform)	ja	ja	ja	ja	ja	ja	ja	ja
Zusätzliche Hardware	nein	nein	nein	nein	nein	ja	ja	nein
Nutzung	WWW/ E-Mail	WWW	E-Mail	WWW	WWW	kein Internet	kein Internet	WWW/ Email

Tabelle 12: Bewertung von Zahlungssystemen nach technischen Kriterien

Organisatorische Kriterien (Stand Oktober 1996)	Ecash	Net-Cash	First Virtual	Cyber Cash	Net Cheque	Mon-dex	CAFE	Tele-Counter
Abhängigkeiten des Anbieters	nein	nein	ja	nein	nein	nein	nein	nein
Abhängigkeiten des Nachfragers	ja	ja	nein	ja	ja	nein	nein	nein
Systemoffenheit	ja[52]	ja	nein	nein	ja	nein	ja	nein
Geldverlust möglich	ja[53]	ja	nein	nein	ja	ja	ja	nein

Tabelle 13: Bewertung von Zahlungssystemen nach organisatorischen Kriterien

Die *Abhängigkeiten* der Teilnehmer beider SmartCard-Systeme wurde verneint, da durch die physische Existenz des Verkäufers und Käufers am Verkaufsort nicht auf eine Lieferung und Zahlung vertraut werden muß. Wie dieses Systeme für die Internet-Nutzung entwickelt werden, bleibt abzuwarten. Durch die Kontenbindung und die Zahlungsausführung direkt durch den Finanzintermediär ist bei den Systemen First Virtual, CyberCash und dem TeleCounter Geldverlust nicht möglich. Begründung hierfür ist, daß sich das Geld nicht lokal auf dem Rechner befindet und versendete Zahlungsversprechen verschlüsselt übertragen werden.

Die nächste Tabelle geht auf die betriebswirtschaftlichen Beurteilungskriterien ein. Im Bereich der Kosten konnte nicht immer eine Angabe gemacht werden, da keine Informationen verfügbar waren, bzw. sich das jeweilige System noch nicht im kommerziellen Einsatz befindet (- = keine Angabe).

Betriebswirtschaftliche Kriterien (Stand Oktober 1996)	Ecash	Net-Cash	First Virtual	Cyber-Cash	Net-Cheque	Mon-dex	CAFE	Tele-counter
Zeitpunkt der Zahlung	pay-now	pay-now	pay-later	pay-later	pay-later	pre-paid	pre-paid	pay-now
Art der Zahlung	cash	cash	credit	credit	cheque	debit	debit	cash
TA-Kosten Anbieter (ohne Kommunikationskosten)	2-3%[54]	-	$0.29 +2%	$0.05[55] +Fixum	-	-	-	-
TA-Kosten Nachfrager (ohne Kommunikationskosten)	4-5%[56]	-	-	-0-	-	-0-	-	-
Monatliche Gebühren Anbieter	$5-25	-	$2	-	-	-	-	-

[51] Bei der Mark Twain Bank müssen die Teilnahmebedingungen ausgedruckt, unterschrieben und per Post zugesandt werden, weiterhin muß eine Überweisung auf das Konto erfolgen.

[52] Momentan ist die Systemoffenheit bei Ecash durch die fehlende Multibanken-Fähigkeit begrenzt; Kunden, die z.B. an dem Pilotprojekt der Deutschen Bank teilnehmen, können ihre Währung nur bei Ecash-Shops die der Deutschen Bank angeschlossen sind, ausgeben. Laut Marcel van der Peijl (Digicash, Amsterdam) wird jedoch an der Multibanken-Fähigkeit gearbeitet.

[53] Bei Zahlungssystemen auf Basis elektronischer Münzes ist es prinzipiell möglich, die lokalen Münzfiles versehentlich zu löschen; entgegenwirkend können von Zeit zu Zeit Sicherheitskopien der Dateien erstellt werden. Münzdateien können auch durch einen Plattencrash verlorengehen.

[54] Dieser Prozentsatz bezieht sich nicht direkt auf die Transaktion. Der Anbieter muß aber bei Einlösung des Geldes (Gutschrift auf realem Konto) eine Gebühr in dieser Höhe bezahlen.

[55] Die Gebühr für die Kartenautorisierung beträgt $0.05.

[56] Der Nachfrager muß bevor er einen Einkauf ausführen kann das Geld von der Münztransfer-Stelle auf seinen Rechner laden, wobei die Gebühr 4-5% des abgehobenen Betrages beträgt.

Betriebswirtschaftliche Kriterien (Stand Oktober 1996)	Ecash	Net-Cash	First Virtual	Cyber-Cash	Net-Cheque	Mon-dex	CAFE	Tele-counter
Monatliche Gebühren Nachfrager	$1-5	-	$2	-	-	£1,50[57]	-	-
Mehrere Währungen möglich	nein	ja	ja	ja	ja	ja	ja	ja
Übertragbarkeit des Geldes	ja	ja	nein	nein	ja	ja	ja	ja
Kommerzielles Entwicklungspotential	ja	nein	ja	ja	nein	ja	nein	ja
Akzeptanzstellen - Finanzinstitute	3	keine	Issuer[58]	24[59]	keine	18	keine	(2)
Akzeptanzstellen - Verkaufsstellen	34[60]	keine	>1.700 [61]	58	keine	>600[62]	keine	keine
Eignung für Micropayments	ja	ja	nein	nein	nein	ja	ja	nein
Eignung für immaterieller Güterkauf >SFr. 50	ja	ja	ja	ja	ja	ja	ja	ja
Eignung für materieller Güterkauf	nein[63]	nein	ja	ja	ja	ja	ja	ja

Tabelle 14: Bewertung von Zahlungssystemen nach betriebswirtschaftlichen Kriterien

Die Gestaltung der Kosten für die Systeme NetCash und NetCheque bleibt abzuwarten. Bei den SmartCards fallen diverse Gebühren beim Aufladen der Karte an.

Abschließend findet die Bewertung der benutzerbezogenen Kriterien statt:

Benutzerbezogene Kriterien	Ecash	Net-Cash	First Virtual	Cyber-Cash	Net-Cheque	Mon-dex	CAFE	Tele-Counter
Akzeptanz/Vertrauen in das System	ja	nein	ja	ja	nein	ja	ja	nein
Anonymität Kunde gegenüber der Bank/AS	ja	ja	nein	nein	nein	nein	ja	nein
Anonymität Kunde gegenüber dem Verkäufer[64]	nein	nein	nein	nein	nein	(ja)	(ja)	nein
Risiken für den Anbieter	nein	ja	nein	nein	ja	nein	ja	ja
Risiken für den Nachfrager	nein	ja	ja	nein	ja	nein	ja	ja
Risiken für Finanzinstitute	ja	ja	ja	ja	ja	ja	ja	ja
E-Mail-Liste für Diskussionsrunde	ja	nein	ja	nein	nein	nein	nein	nein
Help-Hotline zum Systemanbieter	ja	ja	ja	nein	ja	nein	nein	ja

Tabelle 15: Bewertung von Zahlungssystemen nach benutzerbezogenen Kriterien

Die Anonymität der SmartCard-Systeme ist nur gewährleistet, wenn ein immaterielles Gut über das Internet bezogen wird, die Bewertung mit „(ja)“ erfolgte, da SmartCards momentan beim herkömmlichen Kauf auch bei materiellen Gütern Anonymität gewährleisten (wie bei Bargeld).

Generell bestehen wirtschaftliche Risiken für die Anbieter, da elektronische Zahlungssysteme immer mit Aufwendungen verbunden sind und sich keines der Produkte als Standard etabliert hat. Bei den

[57] Wenn die Karte per Telefon aufgeladen wird, kommen noch Telefongebühren hinzu.
[58] Als Akzeptanzstellen kommen alle VISA und Mastercard-Issuer in Betracht.
[59] vgl. http://www.cybercash.com/cybercash/banks/merch_banks.html:
18 Banken und 6 Finanzdienstleistungs-Agenten
[60] Mark Twain Bank: 34 Shops (Merita Bank: 11 Shops ; Ecash: 79 Trial-Shops)
[61] vgl. http://www.fv.com/infohaus/index.html
[62] 600 Verkaufsstellen gibt es allein bei dem Swindon Test
[63] Da keine offiziellen Quittungen bzw. Bestätigungen seitens der Bank erfolgen ist der Zahlungsnachweis zu späterem Zeitpunkt schwer möglich.
[64] Der Verkäufer erhält mindestens die IP-Adresse des Rechners, der am Internet angeschlossen ist.

Anbieter-Risiken ist der Punkt „Server-Sicherheit“, der individuell von den getroffenen Vorkehrungen vor Ort abhängig ist, nicht in die Beurteilung eingeflossen. Bei den Systemen, deren Felder mit „ja“ gefüllt sind, war der Grund die mangelnde kommerzielle Benutzung. Die persönliche Sicherheit und das wirtschaftliche Risiko waren „k.o. - Kriterien“ für die Bewertung der *Nachfrager-Risiken*.

9 Analyse und Bewertung von Zahlungsprotokollen

Im Kapitel Analyse und Bewertung von Zahlungsprotokollen wird eine Abgrenzung von Zahlungsprotokollen zu den elektronischen Zahlungssystemen dargestellt. Ferner werden einige bekannte und wichtige Zahlungsprotokolle beschrieben, die im abschließenden Unterkapitel beurteilt werden.

9.1 Einleitung

9.1.1 Abgrenzung zu elektronischen Zahlungssystemen

Die bisher beschriebenen Zahlungssysteme liegen, eingeordnet in das OSI-Referenzmodell, auf der Anwendungsebene (OSI-Schicht 7). Die meisten sind mit einer graphischen Benutzeroberfläche implementiert und sind somit einfacher in der Handhabung als die Zahlungsprotokolle, die eine technische Spezifikation darstellen. Zahlungsprotokolle können in Transportprotokolle (z.B. SEPP) und Anwendungsprotokolle (z.B. S-HTTP) aufgeteilt werden [Anderer95]. Die in diesem Kapitel beschriebenen Protokolle können direkt für den Zahlungsverkehr im Internet verwendet werden oder gehen als Basisprotokolle in andere Zahlungssysteme ein.

9.2 Zahlungsprotokolle

9.2.1 S-HTTP (Secure Hypertext Transfer Protocol)

S-HTTP wurde im Herbst 1994 von EIT (Enterprise Integration Technologies), vom National Center for Supercomputing Applications (NCSA) und RSA als sicherheitssteigernde Version von HTTP entwickelt, indem es HTTP-Nachrichten kapselt. Es befindet sich ebenso wie HTTP auf der Anwendungsebene, gilt als allgemeines WWW-Sicherheitsverfahren und wird auch für die sichere Übertragung von Zahlungsinformationen verwendet [Janson/Waidner96b]. Es unterstützt Authentifikation von Interprozeßkommunikationen, Nachrichtenintegrität und Non-Repudiation (Nicht-Abstreitbarkeit) des Ursprungs[65].

Das Protokoll beinhaltet die RSA-Kryptographie und Kerberos-basierende Sicherheitsmechanismen. Im Rahmen der Anwendung werden auch andere Kryptographie-Mechanismen zur Auswahl gestellt (z.B. PGP, PEM). Zu HTTP besteht Kompatibilität; wenn nur der Client bzw. Server S-HTTP unterstützt, kann dennoch in Form von ungeschützten Verbindungen kommuniziert werden.

[65] vgl. http://www.eit.com/projects/s-http/

9.2.2 iKP (Internet Keyed Payment Protocols)

Bei iKP handelt es sich um eine Zahlungsprotokollfamilie, die auf der RSA-Kryptographie basiert (Schlüssellänge 1024 Bit bzw. 768 Bit) und von der Forschungsabteilung der IBM Zürich und Yorktown anfangs 1995 entwickelt wurde [Janson/Waidner96a]. Die Architektur ermöglicht, daß drei oder mehr Teilnehmer an einer Session teilnehmen und der Zahlungstransfer direkt über Konten bei Banken oder anderen Finanzorganisationen abgewickelt wird. Die vorhandene Finanz-Infrastruktur soll dabei für die Zahlungsautorisierung und das Clearing verwendet werden. iKP unterstützt Kreditkarten-/Debitkarten-Transaktionen und elektronisches Scheck-Clearing, jedoch kein Electronic Cash [Linehan/Tsudik95][66].

Das Protokoll wurde in verschiedenen Varianten (1KP, 2KP und 3KP) entwickelt, die sich durch verschiedene Sicherheitslevel unterscheiden. Die Variante 3KP ist die umfangreichste, in welcher ein Zahlungsprozeß-Beteiligter einen elektronisch signierten Beweis für seinen relevanten Anteil am Zahlungsvorgang erhält [Janson/Waidner96b].

iKp ist plattformneutral. Um Sicherheitsrisiken zu minimieren wurden mehrere paarweise benutzbare Kanäle entwickelt, so daß die sensitiven Informationen direkt zum Zuständigen gesendet werden können und nicht den Umweg über Dritte machen müssen. Alle Parteien haben eine PIN zur Bestätigung der Zahlungsautorisation. Abhängig vom Bedarf bezieht das Protokoll ein, zwei oder drei öffentliche Schlüssel mit ein. Die akquirierende Bank hat in jedem Fall ein öffentlich-privates Schlüsselpaar, um die vertraulichen Informationen wie z.B. Kreditkartennummern und unterzeichnete Autorisierungsnachrichten zu erhalten und entschlüsseln.

Die Zielsetzungen von iKP sind ein Höchstmaß an Sicherheit für die Beteiligten, die Standardisierung des Mechanismus und der Semantik bei Mehrparteien-Zahlungssitzungen zu erlangen und die bestehende Finanzinfrastruktur einzubeziehen [Janson/Waidner96b]. Im ersten Halbjahr 1996 wurde der iKP Prototyp als Basis für limitierte Versuche fertiggestellt und soll sowohl in Europa als auch in Japan getestet werden. Eine Weiterentwicklung von iKP ist nicht geplant, da zur gleichen Zeit das Protokoll SET entwickelt wurde, welches iKP ablösen wird.

Detaillierte Informationan über iKP liefern die WWW-Seiten:

http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html
http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP_overview.html

9.2.3 STT (Secure Transaction Technology)

Das STT-Protokoll wurde von Microsoft und VISA zur Unterstützung von Zahlungen und Kreditkarten-Transaktionen über elektronische Netzwerke entwickelt, wobei fast komplett auf Standards (z.B. bei den Zertifizierungsformaten) verzichtet wurde. Die Entwicklung „hinter verschlossenen Türen“ erklärt, daß es bis heute keine bedeutende Diskussion über dieses Produkt gegeben hat [Janson/Waidner96a].

[66] vgl. http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/draft-tsudik-ikp-00.txt (Internet draft)

Ebenso wie iKP ist STT in die SET-Spezifikation miteingeflossen. Dadurch erübrigt sich eine Weiterentwicklung dieses Protokolls. In die Bewertung der Zahlungsprotokolle in Kapitel 5.3 wird STT daher nicht aufgenommen.

Die Spezifikation kann von den WWW-Seiten

http://www.visa.com und
http://www.microsoft.com

heruntergeladen werden.

9.2.4 SEPP (Secure Electronic Payment Protocol)

Dieses Protokoll wurde von MasterCard, IBM, Netscape, CyberCash und GTE entwickelt. Bestandteile des Protokolls sind die Erfahrungen mit CyberCash, das Protokoll iKP und dem „Secure Courier“ von Netscape [Reif96].

Durch die Entwicklung des SET-Protokolls, in welches auch die SEPP-Spezifikation eingeflossen ist (siehe Abbildung 5.1) wird das Protokoll voraussichtlich nicht weiterentwickelt werden. Jedoch werden die Protokoll-Funktionalitäten und die Eignung für den Zahlungsverkehr in dem Projekt JEPI[67] untersucht.

Nachfolgende Graphik zeigt den Entwicklungsrahmen von SEPP und anderen Zahlungsprotokollen:

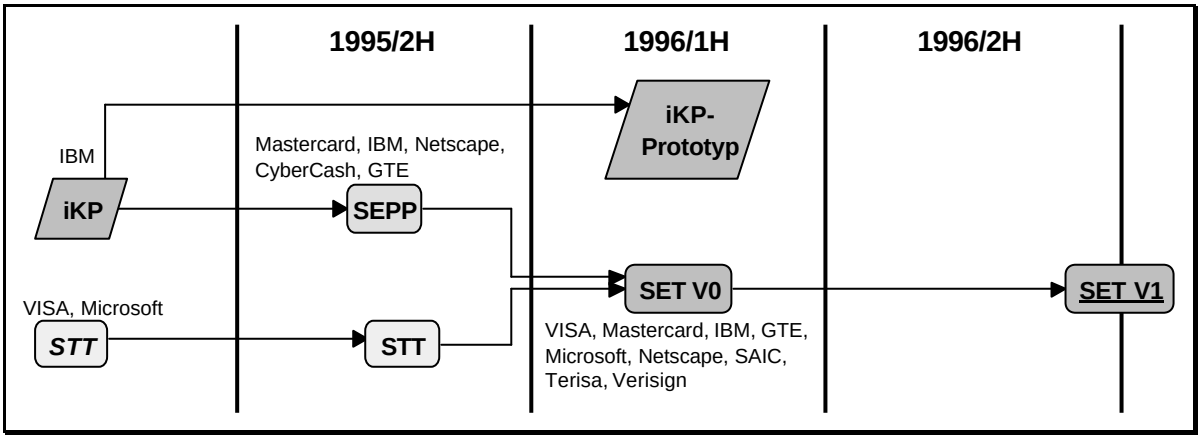

Abbildung 9.1: Historie von Zahlungsprotokollen [Waidner96b]

9.2.5 SET (Secure Electronic Transactions)

VISA und MasterCard haben dieses Protokoll mit der Zielsetzung entwickelt, sichere Kreditkarten-Transaktionen über offene Netzwerke zu ermöglichen. Die Spezifikation kann für Bankkarten-Zahlungen verwendet werden oder sie kann von Software-Herstellern als Grundlage zur Erstellung von Zahlungs-Software dienen[68]. Im Februar 1996 wurde SET zum offiziellen Standard erklärt. GTE, IBM, Microsoft, Netscape Communications Corp., SAIC, Terisa Systems und VeriSign unterstützen VISA und MasterCard bei der Entwicklung von SET.

[67] siehe Kapitel 6.1.2
[68] Die SET-Spezifikation ist auf der folgenden Web-Page verfügbar: http://www.visa.com/cgi-bin/vee/sf/set/intro.html

SET beinhaltet nachfolgend aufgelistete Features[69]:

⇒ Vertrauen in die Informationsversendung durch Nachrichtenverschlüsselung
⇒ Datenintegrität durch digitale Signaturen
⇒ Kartenhalter-, Verkäufer- und Kontenauthentifikation durch digitale Signaturen und Zertifikate
⇒ Interoperabilität durch spezielle Protokolle und Nachrichtenformate

VISA und MasterCard werden SET im vierten Quartal 1996 testen[70], so daß die teilnehmenden Banken ihren Karteninhabern voraussichtlich per 1. Januar 1997 diesen Service anbieten können[71] (siehe Abbildung 5.1). In einer späteren Version von SET werden auch SmartCard-Zahlungstransaktionen möglich sein[72]. Da SET mit Zertifikaten arbeitet, sind Trust Center und eine Zertifizierungshierarchie, wie sie in [Federrath/ Jerichow/ Pfitzmann/ Pfitzmann95] beschrieben wird, notwendig.

Projekte/Produktentwicklungen mit SET[73]:

- Fujitsu Ltd., Hitacht Ltd. und NEC Corporation werden gemeinsam ein System entwickeln, welches elektronische Zahlungen über das Internet basierend auf SET abwickelt[74]. Es handelt sich dabei um ein Projekt der japanischen Regierung[75].
- VeriSign stellt auf seinem Web-Server[76] ein Entwicklungs-Center zur Verfügung, welcher SET-Anwendungsentwicklern bei ihren Produktentwicklungen unterstützt, indem er ihnen SET-Zertifikate zur Verfügung stellt[77].
- Projekte für SET-basierte Anwendungen (z.B. Payment Gateway) wird auch die R3 Sicherheitstechnik AG in Zürich durchführen[78].
- VeriFone wird auf Basis von SET die Payment Transaction Application Layer (PTAL) entwickeln, die vorhandene Zahlungsoptionen wie z.B. Credit (pay-later), Debit (pay-before), Electronic Cash, Micropayments und SmartCards unterstützt [VeriFone], [Tiedemann96]. Komponenten dieser Lösung sind das Pay Window, Virtual Terminal und Internet Gateway.
- COST (Computer Security Technology, Schweden) entwickelt ein vollständiges SET-System für „Nicht-US-Länder“ welches die CA des Clients/Servers, den SET Payment Server für die Bank, den Anbieter (inklusive dem Payment Gateway) und den SET Payment Client für den Karteninhaber beinhaltet. Eine erste Version dieser operationalen Module wird voraussichtlich im März 1997 veröffentlicht[79].
- JavaSoft wird im Rahmen des Java Electronic Commerce Framework (JECF) SET neben SmartCards, elektronischen Schecks, Coupons, u.a. als Bestandteil ihrer Lösung involvieren[80]. Ziele des JECF sind beispielsweise Integration von Einkaufsprozessen in den WWW-Browsing-Prozeß, Erstellung einer offenen, erweiterbaren Plattform für die Bereiche Einkäufe, Banking, Personal- und professionelles Finanz-Management, u.a.[81]

[69] vgl. SET Specification, Book 1: Business Description, DRAFT for public comment, February 23, 1996
[70] vgl. VISA, *MasterCard to test SET in fourth Quarter*, Internet Week via NewsNet, 29.07.96; publiziert in „e-payments“-Diskussionsliste von Tom Wills am 01.08.96.
[71] lt. Tony Lewis, Projektmanager VISA International Service Association, SET-Diskussionsliste am 24.06.96
[72] lt. Tony Lewis, Projektmanager VISA International Service Association, SET-Diskussionsliste am 10.09.96
[73] Nachfolgende Aufzählung erhebt keinen Anspruch auf Vollständigkeit.
[74] lt. Tom Wills, CommerceNet, „e-payments“-Diskussionsliste am 26.07.96
[75] lt. Kosuke Imai, SET-Diskussionsliste vom 26.07.96
[76] vgl. http://digitalid.verisign.com:8001/
[77] lt. getSET Development Center, VeriSign, SET-Diskussionsliste vom 26.07.96
[78] lt. Armin Müller, SET-Diskussionsliste vom 30.07.96
[79] lt. Sead Muftic, COST Schweden, SET-Diskussionsliste vom 25.07.96
[80] lt. Ted Goldstein, Chief Java Commerce Officer, SET-Diskussionsliste vom 28.07.96;
[81] vgl. http://java.sun.com:80/products/commerce/doc.white_paper.html

- Die PBS[82] (Dänische Firma für Zahlungssysteme), MasterCard, Europay und IBM werden in Dänemark ein Pilotprojekt mit einer SET-basierten Zahlungslösung durchführen[83]. Ende des Sommers 1996 wird die IBM Dänemark SET und das notwendige Zubehör bei PBS implementieren, so daß laut PBS-Publikation[84] sichere Kreditkarten-Transaktionen noch in diesem Jahr möglich sind.
- RSA entwickelt ein „SET Toolkit Suite", dessen endgültiges Release im vierten Quartal 1996 käuflich zu erwerben sein wird. Die Preise betragen US$ 25.000 für das Karteninhaber-Toolkit, US$ 50.000 für das Anbieter-Toolkit und US$ 75.000 für das Toolkit des akquirierenden Finanzintermediärs[85].

9.2.6 SSL (Secure Socket Layer)

Das Protokoll SSL wurde von der Firma Netscape Communications entwickelt und hat sich durch die Implementierung in den Produkten Netscape Browser und NetSite Commerce Server als eine Art Standard für verschlüsselte Datenübertragung über das Internet etabliert [Reif96]. Die erste Version wurde Ende des Jahres 1994 eingeführt. Es unterstützt beliebige TCP/IP-basierte Protokolle wie beispielsweise ftp, gopher und telnet.

Innerhalb des OSI-Schichtenmodells ist SSL auf der Session-Layer einzuordnen. Es unterstützt Software-Entwickler von TCP/IP-Anwendungen durch die Nutzung fortgeschrittener Sicherheits-Features [Schonhardt95]. Das Sicherheitsprotokoll ermöglicht einen sicheren Verbindungsaufbau zwischen Browser und Server, ist jedoch auf zwei Parteien limitiert [Waidner96a]. Es sollen Lauschangriffe und das Zurückhalten oder Fälschen von Nachrichten verhütet werden. Die Authentifikationen werden via Zertifikate abgehandelt[86]. Secure Socket Layer übernimmt laut [Cameron96, 224], [Ruf96] und [Flohr96]:

- Datenverschlüsselungen,
- Server-Authentifizierungen,
- optionale Client-Authentifizierungen,
- Nachrichtenintegrität,
- Vertraulichkeit der Datenübermittlung und
- Non-Repudiation des Datenaustausches

Mit dem RC4-Verschlüsselungsalgorithmus (gewöhnlich 40 Bit Schlüssellänge; 128 Bit im US-Binnenmarkt) von RSA werden die Daten verschlüsselt. Generell gesehen haben „Paketsniffer" beim Abhören einer SSL-Verbindung wenig Chancen; jedoch schließt die Verkürzung der Schlüssellänge auf 40 Bit diese Möglichkeit nicht ganz aus [Reif96]. Janson und Waidner bezeichnen die exportierfähigen Protokolle als „zweitklassige" Technologien und halten das Interesse von Banken, Verkäufern und Kunden an solchen für fragwürdig [Janson/Waidner96a] [Janson/Waidner96b].

Mehr Informationen über SSL sind ersichtlich auf der WWW-Seite:

http://home.netscape.com/newsref/std/SSL.html

9.2.7 PCT (Private Communications Technology)

[82] Homepage-URL: http://www.pbs.dk/

[83] lt. Allan Ottosen, Dänemark, „e-payments"-Diskussionsliste vom 22.07.96

[84] *siehe Safe to use credit cards on the Internet already this year*, 18.07.96, URL: http://www.pbs.dk/

[85] lt. Schreiben von Tim Matthews (RSA) am 08.06.96

[86] vgl. http://www.twg.com/emissary/secure.html

PCT ist eine Spezifikation von Microsoft, die eine Erweiterung zu SSL darstellt und Ende des Jahres 1995 veröffentlicht wurde [Bhimani96]. Sie unterstützt sichere Datenkommunikation durch Verschlüsselung. Mit dem Microsoft Internet Explorer Version 2.0 kann private Kommunikation über das Internet erfolgen.

Innerhalb des OSI-Referenzmodells ist PCT wie SSL auf der Session-Layer zu finden. Das Protokoll ermöglicht Server-Authentisierung, Verschlüsselung und Datenintegrität, jedoch keine Non-Repudiation [Janson/Waidner96a].

9.2.8 Millicent Protokoll

Das Millicent Protokoll wurde von Digital Equipment als Abrechnungsmöglichkeit für Kleinstbeträge im Cent-Bereich entworfen [Flohr96]. Broker übernehmen die Kontenführung vom Anbieter und Kunden und erstellen die Berechtigungsscheine für die Kunden. Die kumulierten Beträge, die auch eine Broker-Gebühr beinhaltet, kann der Kunde dann per elektronischen Zahlungsmitteln oder auf herkömmlichem Weg bezahlen [Reif96]. Die Broker dienen somit als Accouting-Intermediäre zwischen den Kunden und den Anbietern, wobei sich Digital Equipment als Broker seriöse finanzielle Institutionen wie VISA, MasterCard, Banken oder auch große Internet- oder Online-Service Provider wie AOL oder CompuServe vorstellen kann [Glassman/u.a.95].

Die Überprüfung auf Mehrfachausgaben der Scheine übernimmt der Verkäufer selbst, somit entfällt ein zentraler Server. Es werden symmetrische Verschlüsselungsverfahren verwendet, das Protokoll bietet keine Anonymität [Janson/Wayner96]. Aufwendige Kryptographie-Mechanismen werden wegen der geringen Beträge nicht angewandt.

Das System wurde bisher nicht kommerziell genutzt, daher wird das System nicht in die Bewertung in Kapitel 5.3 aufgenommen. Ein interner Test bei Digital über TCP/IP-Netzwerke ergab, daß schätzungsweise eintausend Anfragen per Sekunde validiert werden können [Flohr96]. Weitere Informationen über Millicent (detaillierte Funktionsweise, Inhalte der Berechtigungsscheine, u.a.) sind auf nachfolgender Web-Seite enthalten:

http://www.research.digital.com/SRC/millicent/papers/millicent-w3c4/millicent.html

9.3 Bewertung der Zahlungsprotokolle

Die Bewertung der Zahlungsprotokolle findet im Hinblick auf die Eignung des generischen Zahlungssystems statt. Wie bereits im vorangegangenen Kapitel erläutert, sind einige Protokolle durch die Entwicklung von SET kein Diskussionspunkt mehr. Diese Protokolle (iKP, SEPP und STT) werden mit größter Wahrscheinlichkeit kein großes Marktpotential erlangen.

SET wird sich mit höchster Wahrscheinlichkeit für den Bereich Kreditkarten-Transaktionen durchsetzen. Einerseits wird der umfangreiche Sicherheitsmechanismus, andererseits die finanzielle Kraft von VISA, MasterCard u.a. dafür verantwortlich sein. Die Entwicklungen in diesem Bereich und das allseits große Interesse lassen auf einen großen Marktdurchbruch schließen.

Auch SSL wird zukünftig weiterhin eine große Rolle spielen. Durch die Integration im Netscape Browser wird das Protokoll seine Verbreitung weiter erhöhen. Auch die Tatsache, daß SSL diverse Anwendungsprotokolle unterstützt spricht hierfür.

Parallel werden sich Zahlungsprotokolle, die speziell zur Abwicklung von Micropayment-Einkäufen entwickelt wurden, durchsetzen. Um welches Produkt es sich dabei speziell handeln wird (Millicent, PayWord, MicroMint[87] u.a.) ist noch nicht erkennbar.

[87] PayWord und MicroMint sind zwei einfache Protokolle, welche an der RSA Data Security Conference im Januar 1996 in San Francisco vorgestellt wurden (zitiert in [Bhimani96]).

10 Literaturverzeichnis

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

[Adena91] Adena, K. *TCP/IP*.
In: Schneider, Hans-Jochen (Hrsg.): *Lexikon der Informatik und Datenverarbeitung*. 3. Aufl., München, Wien: Oldenburg, 1991.

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

[Bergdolt96] Bergdolt, Gudrun. *Ehrgeizige Chipkarte will die Welt erobern*. Geldinstitute, 1-2, 1996, S. 24-26.

[Beutelspacher/Hueske/Pfau93] Beutelspacher, Albrecht, Hueske, T., und A. Pfau. *Kann man mit Bits bezahlen?* Informatik-Spektrum, Nr.16, 1993, S. 99-106.

[Beutelspacher91] Beutelspacher, Albrecht. *Kryptologie*. Braunschweig: Vieweg, 1991.

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

[Block/Kingson Bloom/Kutler96] Bloch, Valerie, Kingson Bloom, Jennifer, und Jeffrey Kutler. *Soon, home will be where the Smart Card is*. American Banker, July 24, 1996. Publiziert in: e-payments (Diskussionsliste)

[Cameron95] Cameron, Debra. *Implementing the Internet for Business*. Charleston, South Carolina: Computer Technology Research Corp., 1995.

[Chaum82] Chaum, David. *Blind signatures for untraceable payments*. Advances in Cryptology, Proc. Crypto ´82, New York Plenum 1983, S 199 - 203. Zitiert in: [Beutelspacher/Hueske/Pfau93]

[Chaum87] Chaum, David. *Sicherheit ohne Identifizierung*. Informatik Spektrum, Nr. 10, 1987, S. 262 - 277.

[Deutsche Bank96] Deutsche Bank. *Pilotvorhaben der Deutschen Bank zur Evaluierung eines mediengerechten Internet-Zahlungsmittels*. Anlage 2 zu den Unterlagen des Ecash-Pilotbetriebs, Stand 30. August 1996.

[Federrath/u.a.95] Federrath, Hannes, Jerichow, Anja, Pfitzmann, Andreas, und Birgit Pfitzmann. *Mehrseitig sichere Schlüsselerzeugung*.
In: Trust Center. Proceedings der Arbeitskonferenz Trust Center 95, DuD Fachbeiträge, S. 117-131, Wiesbaden: Vieweg, 1995.

[Finney93] Finney, Hal. *First Reaction to Medvinsky NetCash Proposal.* 17.08.1993, URL: http://www.portal.com/~hfinney/netcash_crit.html

[Fischer95] Fischer, Manfred. *Kampf dem Kleingeld*. WirtschaftsWoche, Nr. 31 vom 27.07.1995, S. 16.

[Flohr96] Flohr, Udo. *Electric Money*. BYTE, Nr. 6, 1996, S. 74 - 84.

[Foremski96] Foremski, Tom. *Payment systems - Revolutionary potential.* Financial Times, 04.09.1996, S. VI.

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

[Garfinkel96] Garfinkel, Simson. *Paying through the Net Virtual credit good at Net sites everywhere*. 29.01.96, URL: http://www.fv.com/gabletxt/sjm2_1_29_96.html

[Glassman/u.a.95] Glassman, Steve, Manasse, Mark, Abadi, Martin, Gauthier, Paul, und Patrick Sobalvarro. *The Millicent Protocol for Inexpensive Electronic Commerce*. 1995, URL: http://www.research.digital.com/SRC/millicent/papers/ millicent-w3c4/millicent.html

[Hitachi93] Hitachi Research Institute. *Payment Systems - Strategic Choices for the Future*. Institute of Advanced Business Systems Hitachi, Ltd. (Hrsg.), USA, F.I.A. Financial Publishing Co.: 1993.

[Jansen95] Jansen, Christoph. *Zahlungsprozesse im Internet.* Diplomarbeit, Universität St. Gallen, Herbst 1995.

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

[Janson/Waidner96b] Janson, Phil, und Michael Waidner. *Elektronische Zahlungssysteme*. Computerworld, Nr. 21/1996, S. A6, A8, A22.

[Janson95] Janson, Phil. *Internet Keyed Payment Protocols (iKP)*. Internet draft, Juli 1995, URL: http://www.zurich.ibm.com/Technology/Security/extern/ ecommerce/iKP_overview.html

[Klein95] Klein, Stephan. *Die elektronische Geldbörse zwischen Technik und organisatorischer Anforderung*. Information Management, Nr. 4, 1995, S. 72-79.

[Krähn93] Krähn, Josef. *Rechtliche Rahmenbedingungen eines Electronic Data Interchange: eine institutionenökonomische Analyse*. Lehmann, Michael (Hrsg.). München, VVF: 1993.

[Lindemann96] Lindemann, Markus. *Internet-Dienste für den Elektronischen Datenaustausch (EDI) - Anwendungsbeispiele aus technischer Sicht*. Arbeitsbericht IM HSG/CCEM/34, Universität St. Gallen, August 1996.

[Linehan/Tsudik95] Linehan, M., und G. Tsudik. *Internet Keyed Payments Protocol (iKP)*. Internet draft, Juli 1995, URL: http://www.zurich.ibm.com/Technology/Security/extern/ ecommerce/ draft-tsudik-ikp-00.txt

[Martin96] Martin, Andreas. *Die Auswirkungen des Chips auf die Zahlungssysteme der Kreditwirtschaft.* Karten, Februar 1996, S. 32-36.

[Mausberg95] Mausberg, Paul. *Die elektronische Abwicklung des Zahlungsverkehrs privater Kunden auf Basis eines standardisierten Nachrichtenaustauschs*. In [Schmid95a].

[Oesterle93] Oesterle, H., Saxer, R., und T. Hüttenhain. *Organisatorisches Monitoring als Grundlage für das Business Process Redesign*. Arbeitsbericht IM2000/CCEM/2, Universität St. Gallen, April 1993.

[Raudszus96] Raudszus, Frank. *Electronic Payment via Cybercash*. NET, April 1996, S. 59.

[Reif96] Reif, Holger. *Cyber-Dollars: Elektronisches Geld im Internet.* C´t, Nr. 5, 1996, S. 144-149.

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

[Sperlich96] Sperlich, Tom. *Bündel, Scheine und Münzen*. C´t, Nr. 7, 1996, S. 98-101.

[Steiner/Teixeira90] Steiner, T., und D. Teixeira. *Technology in Banking*. Homewood, I11., 1990.
Zitiert in: Wieland, Bernhard. *Telekommunikation und vertikale Integration*. Heidelberg: Physika, 1995.

[Straub90] Straub, Eduard. *Electronic Banking : Die elektronische Schnittstelle zwischen Banken und Kunden*. Bern, Stuttgart: Haupt, 1990.

[Stumpf96] Stumpf, Thorsten. *Entwurf und Implementierung eines Benutzungsprotokoll- und Abrechnungssystems für WWW Server*. Diplomarbeit FH Technik Mannheim, 1996.

[Tanaka96] Tanaka, Tatsuo. *Possible Economic Consequences of Digital Cash*. fist monday, URL: http://www.firstmonday.dk/issues/issue2/ digital_cash/index.html

[Tiedeman96] Tiedeman, Andrew J.E. *Sicheres Shopping im Internet.* Online Direct, Nr. 1, 1996, S. 20-21.

[VeriFone] VeriFone. *Making Internet Payment Open Secure Convenient* (Broschüre), 1995.

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

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

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

[Weisman/Trevino/ Sweet96] Weisman, David, Trevino, Victor, und Susan, Sweet. *Payments on the Web*. 01.03.1996. Forrester Reseach Inc., URL: http://www.forester.com/