

Zahlungsverkehr via Internet in der Schweiz

Semesterarbeit

Lehrstuhl für Betriebswirtschaft
ETH Zürich
betreut durch Prof. A. Seiler
und Christoph Lukesch

Martin Näf
Auf der Mauer 19
8001 Zürich

Oliver Separovic
Narzissenstrasse 9
8006 Zürich

10. Juli 1998

Vorwort

Die vorliegende Semesterarbeit entstand im Sommer 1998 am Lehrstuhl für Betriebswirtschaft der ETH Zürich unter der Leitung von Prof. A. Seiler. Das Thema "Handel im Internet" hat in der Schweiz erst seit Anfang dieses Jahres an Bedeutung gewonnen, entsprechend bescheiden ist die Anzahl der Anbieter und der erzielte Umsatz. Insbesondere fehlen die grossen Detaillisten wie Coop und Migros. Im Verlauf des Jahres, sowie in den folgenden zwei bis drei Jahren dürfte der Handel, und damit auch der Zahlungsverkehr, eine ungleich grösse Wichtigkeit bekommen.

Für die Möglichkeit, diese aktuelle und spannende Arbeit schreiben zu können, möchten wir uns bei Prof. A. Seiler und unserem Assistenten Ch. Lukesch freundlich bedanken.

Einen speziellen Dank geht an alle Firmen, welche uns mit Ratschlägen und Informationen unterstützt haben. Speziell erwähnen möchten wir die Swiss NetPay AG und die Reimer AG, welche uns ihr System demonstriert hat und bereitwillig Auskunft rund um den elektronischen Zahlungsverkehr in der Schweiz gab.

Zürich, im Juli 1998

Oliver Separovic
Martin Näf

Zusammenfassung

Der vorliegende Bericht erläutert den Zahlungsverkehr via Internet in der Schweiz. Dabei werden sowohl betriebswirtschaftliche wie auch technische Aspekte der aktuellen und der in naher Zukunft verfügbaren Systeme beleuchtet.

Übersicht

Kapitel 2 gibt eine Übersicht über den herkömmlichen Zahlungsverkehr. Dabei wird zuerst das Grundmodell "Abheben - Zahlung - Gutschrift" eingeführt, welches jedem Zahlungssystem zugrunde liegt. Über den Zeitpunkt der drei Schritte werden anschliessend die verschiedenen Basissysteme (Debit-, Pay-now- und Pay-later-System) eingeführt und anhand von Beispielen erläutert. Weiter wird zwischen reinen Buchungssystemen und solchen, bei welchen ein Wert das Bankensystem effektiv verlässt, unterschieden.

Im zweiten Teil dieses Kapitels wird auf die technische Umsetzung im Internet eingegangen. Dabei ist einerseits das Problem der Authentifizierung, der eindeutigen Identifikation der an einer Transaktion beteiligten Parteien, zu lösen, andererseits muss ein Minimum an Abhörsicherheit geschaffen werden. Beide Probleme können mittels kryptographischen Protokollen gelöst werden (Anhang A erläutert die Grundbegriffe). Weiter wird ein Grundmodell für elektronisches Bargeld mit Anforderungen und deren Realisierung vorgestellt.

Erfolgsfaktoren

Im Kapitel 3 werden die Erfolgsfaktoren für Zahlungssysteme identifiziert. Begonnen wird mit einer kurzen Erläuterung der rechtlichen Situation. Hier gibt es noch wichtige offene Punkte wie die Akzeptanz von elektronischen Unterschriften, die Haftungsfrage bei Kreditkartenmissbrauch, sowie nicht zuletzt die Tatsache, dass elektronisches Geld nicht dem Bankengesetz unterstellt ist. Die Kosten sind zurzeit einer der wichtigsten Erfolgsfaktoren. Elektronische Zahlungsmittel verursachen heute wesentlich kleinere Kosten, sowohl für die Banken wie auch für die Händler.

Sicherheit und Vertrauen sind wichtige Aspekte primär aus Sicht der Kunden. So sind Fragen wie Anonymität und Datenschutz zu klären.

In eine ähnliche Richtung zielt auch der Erfolgsfaktor Zeit. Der Kunde will schnell und einfach bezahlen können. Zeit spielt aber auch bei den Kosten für die Banken eine grosse Rolle.

Zuletzt wird auf Qualität und Flexibilität eingegangen. Dies ist sowohl aus Kunden- wie auch aus Händlersicht wichtig. Das zur Verfügung stehende System muss sowohl flexibel wie auch zuverlässig funktionieren, um eine gewisse Akzeptanz erreichen zu können.

Produkte

Im Kapitel 4 werden Produkte für den elektronischen Zahlungsverkehr vorgestellt, welche heute erhältlich oder im Versuchsstadium sind. "First Virtual" ist ein einfaches System für Kreditkartentransaktionen, "SSL" wird als Beispiel eines sicheren Transportprotokolls erwähnt. "SET" schliesslich ist ein System zur sicheren Übertragung von Kreditkarteninformationen. Speziell interessant ist "ecash" als bisher erfolgreichste Implementation von elektronischem Geld.

Markt Schweiz

Im Kapitel 5 wird näher auf den aktuellen Zustand in der Schweiz eingegangen. Dazu wurde eine Umfrage bei Firmen durchgeführt, welche E-Commerce betreiben. Die Resultate werden analysiert und kommentiert. Interessant ist dabei die Tatsache, dass insbesondere der Reduktion von Debitorenverlusten sehr grosses Gewicht beigemessen wird.

Weiter werden drei Anbieter von Internetzahlungssystemen kurz vorgestellt. Es sind dies die Reimer AG, The Blue Window (Swisscom) und die Swiss NetPay AG.

Zukunft

Im Kapitel 6 wird ein kurzer Blick in die Zukunft gewagt. Dieser ist allerdings in hohem Masse spekulativ, da sich das Internet nicht nur technologisch sondern auch ökonomisch zurzeit enorm schnell entwickelt. Sicher ist aber, dass aufgrund des Kostenvorteils die Zukunft dem elektronischen Zahlungsverkehr gehört.

Abkürzungen

ACH	Automated Clearing House
ATM	Automated Teller Machine
BaG	Bankengesetz
EFTPOS	Electronic Funds Transfer at the Point of Sale
ISP	Internet Service Provider
LSV	Lastschriftverfahren
POS	Point of Sale
SET	Secure Electronic Transactions
SIC	Swiss Interbank Clearing
SNB	Schweizerische Nationalbank
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
ZV	Zahlungsverkehr

Inhaltsverzeichnis

1	Einleitung	1
2	Übersicht über den Zahlungsverkehr	3
2.1	Herkömmlicher Zahlungsverkehr	3
2.2	Technische Möglichkeiten im Internet	7
3	Die Erfolgsfaktoren im Zahlungsverkehr	11
3.1	Recht	11
3.2	Kosten und Nutzen des Zahlungsverkehrs	14
3.3	Sicherheit und Vertrauen	19
3.4	Zeit	21
3.5	Qualität und Flexibilität	22
4	Angebote Produkte	23
4.1	First Virtual	23
4.2	SSL	25
4.3	SET	26
4.4	ecash	28
4.5	Andere Projekte	30
5	Internetzahlungsverkehr in der Schweiz	31
5.1	Auswertung der Umfrage	31
5.2	Anbieter von Zahlungssystemen	35
6	Zukunft des Internet-Zahlungsverkehrs	39
A	Kryptographische Grundlagen	41
A.1	Definitionen	41
A.2	Symmetrische Verschlüsselung	43
A.3	Public-Key Kryptographie	44
A.4	Elektronische Unterschriften	44
A.5	Sicherheit	46
B	Fragebogen	49
B.1	Firmen mit elektronischen Zahlungsmöglichkeiten	49
B.2	Firmen ohne elektronische Zahlungsmöglichkeit	54
B.3	Auswertung	57
	Literaturverzeichnis	67

Kapitel 1

Einleitung

Mit dem Wachstum des Internets und der steigenden Anzahl Benutzer hat auch der Begriff *Electronic Commerce* (kurz *E-Commerce*) Einzug gehalten. Er wird als Oberbegriff für eine Reihe elektronischer Instrumente zur Abwicklung von Geschäftstransaktionen übers Internet verwendet. Dabei werden alle Phasen einer Transaktion, von der Werbung, über die Logistik und die Preisfestsetzung, bis hin zur Zahlung, eingerechnet. Der Umsatz im Internethandel lag 1997 bei etwa US\$ 8,5 Mrd. Das Marktforschungsinstitut Forrester Research schätzt das Volumen für 1998 auf US\$ 17 Mrd., also gut das Doppelte – und prophezeit für das Jahr 2002 US\$ 327 Mrd. So beeindruckend diese Zahlen auf den ersten Blick sind, in Relation zu anderen Grössen schrumpfen sie schnell. So entsprechen die 17 Mrd. Umsatz für 1998 etwa dem Jahresgewinn von Migros und Coop zusammen, betreffen jedoch den weltweiten Handel im Internet.¹ Trotzdem wird sich in Zukunft kaum ein Unternehmen erlauben können, nicht auf dem Internet präsent zu sein.

Wie in der Aufgabenstellung verlangt, geht der Bericht nicht auf den gesamten E-Commerce ein, sondern beschränkt sich auf die Phase der Zahlungstransaktion von Privatkunden gegenüber Händlern. Der Zahlungsverkehr der Banken wird dabei nicht betrachtet. Isolierte Prognosen für die Zunahme an Zahlungen übers Internet, d. h. ohne Einbezug des gesamten E-Commerce, sind kaum möglich. So hängt beispielsweise das Aufkommen von Zahlungen via Internet mit dem generellen Zuwachs an Einkaufsmöglichkeiten auf dem Internet zusammen. Nur wenn sich die Anzahl von Direkteinkaufsmöglichkeiten übers Netz vergrössert, gewinnt auch der Zahlungsverkehr via Internet an Bedeutung. Weiter sind nicht alle Produkte zum Verkauf über Internet gleich geeignet, der Verkauf von Büchern und Computern ist zum Renner geworden; der Computerhersteller Dell verkauft weltweit übers Internet 1500 seiner PC's – pro Tag.

Verglichen mit den USA ist die Zurückhaltung in der Schweiz noch relativ gross. Dennoch gibt es einige neue Projekte, die den E-Commerce fördern, wie z. B. die "Elektronische Mall Bodensee"² und "Le Shop"³. Es kann davon ausgegangen werden, dass sich der Verkauf übers Internet auch in der Schweiz mittelfristig zu einem zusätzlichen Standbein für Firmen entwickeln wird. Die Voraussetzungen dazu sind gegeben; so besitzen 50% aller Haushalte einen PC und 90% aller TV-Konsumenten sind an ein Kabelnetz wie Cablecom angeschlossen, welches in den nächsten 2 bis 3 Jahren den Zugang zum Internet via Fernseekabel für alle Kunden ermöglichen wird.

¹Handelszeitung Nr. 14 vom 2. April 1998, S. 56

²<http://emb.net>

³<http://www.leshop.ch>

Wie in jedem anderen Geschäftszweig herrscht auch bei den Zahlungsverkehrs-Produkten ein Konkurrenzkampf untereinander. Die Selektion der geeigneten Produkte erfolgt über Marktanalysen. Der Bericht versucht eine solche Analyse im Zahlungsverkehr vorzunehmen.

Im Kapitel 2 wird zuerst auf die herkömmlichen Produkte eingegangen und deren Vor- und Nachteile gezeigt. Ein Ausflug in die Welt des Internets soll die Möglichkeiten zur Abbildung von herkömmlichen Zahlungsmittel auf den Computer aufzeigen.

Den kritischen Erfolgsfaktoren im Zahlungsverkehr, insbesondere im Zahlungsverkehr via Internet, ist Kapitel 3 gewidmet. Es wird auf die Faktoren Recht, Kosten, Sicherheit und Vertrauen, Zeit und Qualität und Flexibilität eingegangen.

Im Kapitel 4 werden die momentan vorhandenen und für die Schweiz wichtigen Produkte im einzelnen vorgestellt und ihre Stärken und Schwächen besprochen.

Kapitel 5 bespricht und kommentiert die im Rahmen der Arbeit durchgeführte Umfrage. Zudem werden Beispiele einzelner Firmen dargestellt, die Zahlungsverkehr via Internet in der Schweiz anbieten.

Als Abschluss wird versucht, einen Blick in die Zukunft zu werfen. Wird sich der Zahlungsverkehr via Internet durchsetzen? Falls ja, in welchem Zeitraum? Welche Produkte sind im Moment am erfolgsversprechendsten? Einzelne dieser Fragen können heute schon tendenziell beantwortet werden.

Kapitel 2

Übersicht über den Zahlungsverkehr

2.1 Herkömmlicher Zahlungsverkehr

Dieses Kapitel erläutert kurz die wesentlichen Elemente des Zahlungsverkehrs (ZV) und gibt eine Einteilung der wichtigsten ZV-Mittel wieder. Weiter wird auf deren Vor- und Nachteile eingegangen. Wie weiter unten dargestellt wird, ist der ZV via Internet nur eine Adaption neuer, technischer Möglichkeiten an den bisherigen elektronischen ZV.

Die Definition für den *elektronischen Zahlungsverkehr* lautet im folgenden: "Gegenstand des Zahlungsverkehrs ist die unbare Form der Zahlung bzw. der Transport der *Zahlungsinformation*".¹ Dabei ist es sehr wohl möglich, dass am Beginn und am Ende einer Zahlung Bargeld steht.

Der Austausch von Gütern ist seit jeher fester Bestandteil jeder Zivilisation. Erst durch den Tausch wird eine Arbeitsteilung überhaupt möglich. Mit der Zeit wurde sowohl der reine Tauschhandel, als auch der Handel mit Warenbezahlung zu kompliziert, Geld wurde erfunden. Damit konnten Käufe und Verkäufe abgewickelt werden, ohne beidseitig reelle Waren auszutauschen. Neben der Funktion als Tauschmedium dient Geld auch als Recheneinheit und der Wertaufbewahrung.²

Der nächste Schritt in der Entwicklung des ZV war die Erfindung von Scheck³, sowie einiges später die Erfindung von "Plastikgeld" in Form von Kredit- und Debitkarten⁴. Diese Arten von Geldersatz erlauben die Bezahlung ohne Bargeld und sind für den Benutzer im Gebrauch schneller, angenehmer, sicherer und teilweise auch weniger teuer.

2.1.1 Grundkomponenten im ZV

An einer Geschäftstransaktion nehmen grundsätzlich immer ein Käufer und ein Verkäufer teil, welche Waren gegen Geld austauschen. In den meisten existierenden (elektronischen) Zahlungssystemen ist zudem mindestens ein Fi-

¹G. D. Lehmann, "Zahlungsverkehr der Banken", Verlag des Schweizerischen Kaufmännischen Verbandes, Zürich 1992, S. 14

²Prof. Dr. Klaus Spremann, "Wettbewerb und Technologie im Zahlungsverkehr", Verlag Paul Haupt, 1997, S. 171

³Def. Scheck: Anweisung an eine Bank, von einem Konto eine bestimmte Geldsumme an den Scheckinhaber zu bezahlen.

⁴Def. Debitkarte: Karte bei der vor der Bezahlung Geld auf der Karte, bzw. auf dem zugehörigen Konto sein muss.

nanzinstitut⁵ involviert, welches die ausgetauschten Informationen in Geld umwandelt. Üblicherweise wird diese Vermittlerrolle von 2 Banken wahrgenommen, einem Issuer (die Bank des Käufers) und einem Acquirer (die Bank des Zahlungsempfängers/Verkäufers). Zusätzlich überwacht ein Schiedsrichter (der Staat) das Geschehen. Dabei ergeben sich die folgenden Geldflüsse, siehe dazu auch Abbildung 2.1.⁶:

- Vom Issuer zum Käufer durch eine Kontobelastung (z. B. mittels ec-Karte oder Abheben von Bargeld am Bankschalter usw.),
- Vom Issuer zum Acquirer (Interbankenclearing),
- Vom Acquirer zum Verkäufer mittels Überweisung von Geld auf das Konto des Verkäufers.

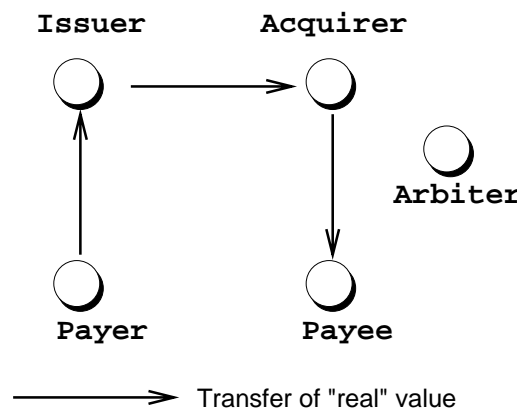


Abbildung 2.1: Grundkomponenten eines Zahlungssystems

Die entsprechenden Systeme für das Interbankenclearing in der Schweiz, das SIC (Swiss Interbank Clearing) und das in sich geschlossene System der Post, sowie SWIFT (Society for Worldwide Interbank Financial Telecommunication) für Meldungsaustausch, werden über eigene Netzwerke abgewickelt. In dieser Arbeit wird nicht weiter darauf eingegangen. Im folgenden werden Banken, Clearingstellen und Kreditkartenunternehmen als Gesamtsystem betrachtet und vereinfacht als Bank bezeichnet.

2.1.2 Zahlungsmodelle

Um eine Übersicht über die vorhandenen Produkte im ZV zu gewinnen, sollen die Zahlungssysteme anhand des Informationsflusses klassifiziert werden. Als erstes wird unterschieden, ob der Informationsfluss *direkt* oder *indirekt* vom Käufer zum Verkäufer läuft.⁷ Im indirekten Fall wird die Zahlungstransaktion von einem der beiden Beteiligten initiiert, der andere wird lediglich von

⁵Normalerweise, aber nicht zwingend, handelt es sich bei den Finanzinstituten um Banken oder Kreditkartenunternehmen.

⁶N. Asokan, Doktorarbeit "Fairness in Electronic Commerce", Universität von Waterloo, 1998, S. 88ff.

⁷N. Asokan, Doktorarbeit "Fairness in Electronic Commerce", Universität von Waterloo 1998, S. 87

seiner Bank über den korrekten Abschluss der Transaktion orientiert. Beispiele dazu sind Überweisungen, Lastschriftverfahren oder elektronische Systeme zwischen Firmen. Direktzahlungen erfolgen u. a. mittels Bargeld oder Kreditkarte.

Als zweites wird anhand des zeitlichen Verlaufs einer Zahlung klassifiziert. Die folgenden Aktionen sind für eine Zahlungstransaktion notwendig:

- Abheben (Käufer bei seiner Bank)
- Bezahlen (Käufer beim Issuer)
- Gutschreiben (Acquirer auf Konto des Verkäufers)

Daraus ergeben sich die folgenden Typen von Zahlungssystemen:

- In einem *pre-paid (debit) Zahlungssystem* hebt der Käufer vor einem Kauf Geld (Bar- oder Buchgeld) von seinem Konto ab.
- *Pay-now Zahlungssysteme* bearbeiten die Zahlung zum Zeitpunkt des Kaufes.
- *Pay-later Zahlungssysteme* erlauben dem Käufer seinen Kauf auf Kredit zu tätigen.

Zusätzlich zur obigen Einteilung kann die Unterscheidung in geldartige Systeme und in Buchungssysteme gemacht werden. Bei geldartigen Systemen verlässt echter Wert in Form von Bargeld, Wertkartensystemen (aufladbar oder nicht) oder digitalem Geld das Bankensystem. Bei Buchungssystemen werden Werte nur innerhalb des Bankensystems verschoben, Beispiele dafür sind ec-DIRECT, Schecks oder Kreditkarten.

2.1.3 Die bestehenden Produkte

Der folgende Abschnitt gibt eine Übersicht über die in der Schweiz gebräuchlichen Produkte, ohne Gewähr auf Vollständigkeit.

- **Bargeld** ist mehr oder weniger universell einsetzbar und wird praktisch überall akzeptiert. Es ist ein pre-paid Zahlungsmittel und kann sowohl für direkte, als auch indirekte Zahlungen verwendet werden. Geld garantiert Anonymität. Die Nachteile liegen in der geringen Sicherheit und der mangelnden Integrierbarkeit in automatisierte Wirtschaftsprozesse.
- **Bancomat und Postomat** werden als Filialautomaten bezeichnet. Die am häufigsten genutzte Funktion ist der Bezug von Bargeld. Es kann zwischen *Cash Dispenser* (Automaten die nur der Geldausgabe dienen) und *Automated Teller Machine (ATM)*, d.h. Automaten mit erweiterten Funktionen wie Kontostandsanzeige, Buchungsmöglichkeiten, etc., unterschieden werden.⁸ Im zeitlichen Verlauf einer Zahlungstransaktion spielen sie nur beim Abheben des Bargelds für einen späteren Kauf eine Rolle. Anonymität ist nur beim Bezahlen, aber nicht beim Abheben gewährleistet.
- **CASH** fällt ebenfalls in die Klasse der pre-pay Zahlungssysteme. Es ist das neueste Produkt im herkömmlichen, elektronischen ZV. Anstelle von Bargeld wird an einem ATM Geld in elektronischer Form auf eine Karte geladen und diese beim Bezahlen verwendet. Ein in die Karte integrierter Chip erlaubt die Speicherung des aktuellen Kartenbetrags. Überwachung ist sowohl beim Kauf als auch bei der Bezahlung möglich.

⁸K. Schaufelberger, "Kartengestützte Zahlungssysteme", Peter Lang AG, 1995, S. 5

- **ec-DIRECT und Postomat-Plus** sind Buchungssysteme, die eine pay-now Zahlung ermöglichen. Sie werden als EFTPOS – Electronic Funds Transfer at the Point of Sale – Systeme bezeichnet. Die Zahlung erfolgt wie bei allen bisher beschriebenen Produkten direkt. Es muss allerdings eine Verbindung zur Bank hergestellt werden, wodurch Wartezeiten entstehen und die Anonymität des Käufers durchbrochen wird.
- **Schecks und Kreditkarten** sind den pay-later Zahlungssystemen zuzurechnen. So wie sie heute verwendet werden, sind sie relativ unsicher, da Fälschungen und Kartenmissbrauch möglich sind. Die Anonymität ist nicht gewährleistet, die Kreditkartenherausgeber können die Transaktionen ihrer Kunden speichern und nachvollziehen. Die beiden Produkte dienen ebenfalls zur direkten Bezahlung.
- **Einzahlungsscheine und Lastschriftverfahren** sind als indirekte, pay-later Produkte zu qualifizieren. Die Bezahlung erfolgt beim Einzahlungsschein durch den Käufer durch Einzahlung am Post- oder Bankschalter oder mittels Zahlungsanweisung. Beim Lastschriftverfahren (LSV) wird dem Käufer auf Aufforderung durch den Verkäufer, genauer durch dessen Bank, der geschuldete Betrag von seinem Konto abgebogen.

Auf Produkte wie Datenträgeraustausch (DTA) und Electronic Data Interchange (EDI) wird im Rahmen dieser Arbeit nicht eingegangen, da diese Produkte nur zum ZV zwischen Firmen eingesetzt werden.

Die Statistik in Abbildung 2.2⁹ zeigt die Entwicklung der Bedeutung der bargeldlosen Zahlungsmittel in der Schweiz.

Instrumente	1992	1993	1994	1995	1996
Über Banken:					
Schecks	47.71	37.21	31.36	26.34	22.19
Debit- und Kreditkarten	8.43	10.57	12.74	14.87	17.16
Papierlose Überweisungen	33,369.00	34,126.00	33,476.89	32,428.90	38,284.87
Direktdebit	.	.	29.77	36.30	41.56
Total	33,425.14	34,173.78	33,550.76	32,506.41	38,365.78
Über die PTT:					
Debitkarten	0.13	0.30	0.68	1.76	2.94
Überweisungen	1,107.25	1,124.47	1,128.85	1,161.67	1,245.73
Total	1,107.38	1,124.77	1,129.53	1,163.43	1,248.67
Gesamt	34,532.52	35,298.55	34,680.29	33,669.84	39,614.45

Abbildung 2.2: Entwicklung des bargeldlosen ZV in der Schweiz (in Mrd. CHF)

Die Bargeldquote¹⁰ lag in der Schweiz 1996 bei 33%¹¹. Die Schweiz ist damit ein typisches Bargeldland, im Gegensatz etwa zu den USA, die im gleichen Jahr eine Quote von 20% aufwiesen.

⁹Committee on Payment and Settlement Systems, "Statistics on Payment Systems in the Group of Ten Countries", Bank for International Settlements, 1996, S. 87

¹⁰Unter Bargeldquote wird das Verhältnis von Bargeld zur gesamten Geldmenge (Bargeld plus Buchgeld) verstanden.

¹¹Ch. Hirszowicz, "Schweizerische Bankpolitik", Verlag Paul Haupt, Bern 1996, S. 346

2.2 Technische Möglichkeiten im Internet

Dieses Kapitel zeigt Möglichkeiten auf, wie der ZV in elektronischen Netzen modelliert und gesichert werden kann. Dabei wird eine Reihe von Begriffen aus der Kryptographie verwendet, welche im Anhang A genauer erläutert werden.

2.2.1 Authentifizierung

Ein Basisproblem fast sämtlicher bargeldlosen Zahlungstransaktionen ist die gegenseitige Authentifizierung. Wird z. B. eine Kreditkartennummer über das Internet versendet, muss festgestellt werden, ob der Kunde auch tatsächlich der rechtliche Inhaber der Karte ist. Im Alltagsgebrauch wird dies mittels Unterschrift sichergestellt, im Internet hingegen herrscht blindes Vertrauen.

Damit auch im elektronischen Umfeld eine Benutzerauthentifizierung stattfinden kann, gibt es mehrere Verfahren:

- **PIN-Codes** sind geheime Passwörter der Benutzer, welche zusätzlich zur Kartennummer übermittelt werden. Dieses System bedingt einen sicheren Kanal, damit ein Gegner nicht mithören kann. Ein Beispiel für dieses System sind die EFTPOS-Terminals.
- **Elektronische Unterschriften** dienen zur Bestätigung einer Zahlungsanweisung. Wichtig ist hier die Einmaligkeit der Transaktionsdaten, damit dieselbe Transaktion nicht mehrfach ausgeführt werden kann (Replay-Attack).
- **Der Aufbau eines sicheren Kanals** erfolgt mittels eines beliebigen Kryptoverfahrens. Dies kann beispielsweise durch Verwendung eines symmetrischen Verschlüsselungsverfahrens geschehen. Gut geeignet sind auch Public-Key Kryptosysteme, eventuell ergänzt durch Zero-Knowledge Beweise zur effizienten Authentisierung.
- **Hardwaremodule** zur Authentisierung werden ähnlich eingesetzt wie die oben genannten Verfahren. Ihr Vorteil ist, dass grössere Schlüssel oder PIN-Codes gespeichert, sowie komplexere Berechnungen ausgeführt werden können.

2.2.2 Elektronisches Geld

Das Zusammenspiel von verschiedenen kryptographischen Verfahren ermöglicht die Realisierung von elektronischem Geld, welches ähnlich wie Bargeld handhabbar ist, gegenüber diesem aber einige Vorteile besitzt. In den folgenden Abschnitten werden verschiedene Anforderungen definiert sowie Realisierungsvarianten aufgezeigt.

Modell

Das Zahlungsmodell bei elektronischem Geld unterscheidet sich nur in wenigen Punkten von jenem mit herkömmlichem Geld. Der wesentlichste Unterschied ist, dass eine elektronische Münze im allgemeinen nur für eine einzige Zahlung verwendet und nicht mehrfach weitergegeben werden kann.

Bei der Verwendung von elektronischem Geld existieren dieselben Schritte wie bei traditionellem Geld:

- **Abheben** einer elektronische Münze von einem Bankkonto. Diese Münze, ein Datenpaket, wird lokal beim Benutzer gespeichert.

- **Bezahlung** in einem Geschäft durch einen Kunden mit einer digitalen Münze.
- **Einzahlung** der Münze durch das Geschäft bei der Bank und Gutschrift des Wertes auf seinem Bankkonto.

Anforderungen

Eine elektronische Münze ist nichts anderes als digitale Information, welche beliebig kopiert werden kann. Damit diese ihre Funktion als Zahlungsmittel wahrnehmen kann, müssen verschiedene Anforderungen erfüllt sein:

- **Fälschungssicherheit** muss bei elektronischen Münzen durch spezielle Vorkehrungen erreicht werden, während bei Banknoten Fälschungen durch physikalische Merkmale (Wasserzeichen, Metallfaden, Spezialpapier, etc.) verhindert werden. Es muss möglich sein, eine ungültige Münze effizient zu erkennen.
- **Einmalige Verwendbarkeit** Mehrfaches Ausgeben derselben Münze (Double-Spending) ist bei digitalem Geld ohne spezielle Vorkehrungen problemlos möglich. Grundsätzlich kann dies nicht verhindert, sondern nur detektiert werden. Double-Spending kann sowohl vom Kunden bei der Bezahlung, wie auch vom Verkäufer beim Einzahlen ins Bankensystem, vorkommen.
- **Anonymität** wird dadurch erreicht, dass Zahlungen nicht nachvollzogen werden können, dies aus Datenschutzgründen. Es soll verhindert werden, dass bei der Einzahlung festgestellt werden kann, welcher Kunde die Münze abgehoben hat.
- **Schutz gegen Kriminalität** Elektronisches Geld kann vollständig anonym gehalten werden. Dies ist aus Sicht der Kunden, welche Wert auf Datenschutz legen, eine legitime Forderung. Gleichzeitig aber wird durch die Anonymität ein grosses Potential für Kriminalität geschaffen. So bietet elektronisches Geld enorme Möglichkeiten zur Geldwäscherei oder auch zur perfekten Erpressung (das Geld kann z. B. in einer Zeitung abgedruckt werden). Es ist daher wünschenswert, dass der Staat oder eine andere, berechnete Instanz auf richterlichen Befehl hin die Anonymität einer Münze aufheben kann.

Realisierung

In den folgenden Abschnitten wird erläutert, wie die oben genannten Anforderungen erfüllt werden können:

- **Abheben** Beim Abheben muss sichergestellt werden, dass die Münze gültig ist. Dies wird durch eine unfälschbare, elektronische Unterschrift der Bank sichergestellt. Weiter muss bereits hier die Münze mit einer eindeutigen Nummer gekennzeichnet werden, damit ein Double-Spending später detektiert werden kann.
Wenn auf Anonymität verzichtet werden kann, darf diese Nummer von der Bank vergeben werden. Möchte der Kunde hingegen die Münze anonymisieren, muss er die Nummer selbst vergeben (die Einmaligkeit wird durch technische Verfahren sichergestellt) und anschliessend die Münze von der Bank blind unterschreiben lassen.
Unterschiedliche Münzbeträge können entweder durch ein zusätzliches

Datenfeld oder durch verschiedene Unterschriften, z. B. ein Public-Key pro Münzwert, der Bank realisiert werden.

- **Bezahlung** Der Händler, der eine Münze annehmen soll, wird zuerst deren Gültigkeit anhand der Unterschrift der Bank verifizieren. Anschließend fragt er die Bank an, ob die Münze bereits ausgegeben wurde (er übermittelt hierzu die ID der Münze). Ist dies nicht der Fall, akzeptiert der Händler die Münze.

Um zu verhindern, dass der Händler die Münze im Namen des Kunden doppelt verwendet, sollte der Kunde die Münze sowie eine ID des Händlers elektronisch unterschreiben. Erst mit diesem Schritt wird die Münze gültig.

Die Überprüfung der ID vor der Bezahlung hat den Nachteil, dass der Händler eine permanente Verbindung zur Bank benötigt, was als Online-Betrieb bezeichnet wird. Zusätzlich wird die Dauer der Transaktion verlängert.

Ein Double-Spending lässt sich bei einem Offline-Betrieb, also ohne stehende Verbindung, grundsätzlich nicht verhindern. Durch spezielle Signaturverfahren kann die Anonymität des Kunden beim Double-Spending aufgehoben werden: Wird die selbe Münze zweifach ausgegeben, lässt sich aus den beiden resultierenden Unterschriften des Käufers die Identität berechnen. Eine einzige Unterschrift gibt hingegen keine Information über die Identität des Kunden preis.

- **Einzahlung** Bei der Einzahlung der Münze prüft die Bank, ob die Münze ungültig ist oder ob sie bereits einbezahlt wurde. Ist dies nicht der Fall, wird der Betrag der Münze dem Händler gutgeschrieben sowie deren ID in die Datenbank der bereits ausgegebenen Münzen eingetragen. Dadurch, dass die Bank bei der Ausgabe die Seriennummer blind unterschrieben hat, lässt sich keine Verbindung zwischen dem Kunden und dem Händler herstellen, womit die Anonymität gewährleistet ist.
- **Datenschutz vs. Kriminalität** Aufhebung der Anonymität kann durch sogenannte key-escrowing Verfahren¹² realisiert werden. Bisherige Bemühungen (z.B. Clipper-Chip) der US-Regierung in diese Richtung sind allerdings an der mangelnden Akzeptanz der Benutzer gescheitert.

¹²Erklärung siehe Literatur

Kapitel 3

Die Erfolgsfaktoren im Zahlungsverkehr

3.1 Recht

Das Internet ist zu einem grossen Teil immer noch ein rechtsfreier Raum. Da das Netz grenzübergreifend funktioniert, sind gesetzliche Einschränkungen einzelner Staaten nur bedingt durchsetzbar.¹

In diesem Umfeld müssen Firmen Investitionen in Hard- und Software tätigen, deren Nutzen durch neue Gesetzgebungen von einem Tag auf den andern in Frage gestellt werden können.² Gerade im ZV, wo weitaus grösserer technischer und finanzieller Aufwand notwendig ist, als bei einer reinen Informationsanwendung, sollte eine rechtliche Sicherheit vorhanden sein, um das Risiko von Fehlinvestitionen zu verkleinern.

Auch aus Konsumentensicht sind gewisse Rechtsgrundlagen wünschenswert. So stehen z. B. Fragen bezüglich Datenschutz oder der Haftung bei Kreditkartenmissbrauch im Raum. Weitere Fragen wie etwa Zollpolitik und Steuern betreffen nicht nur die Schweiz alleine und müssen von supranationalen Organisationen wie der OECD oder der WTO behandelt werden. Der Bericht geht im folgenden den Fragen betreffend digitalen Signaturen, der rechtlichen Situation bei Kreditkartengebrauch und dem Gebrauch von digitalem Geld in der Schweiz nach.

Digitale Signaturen

Das Schweizerische Obligationenrecht (OR) stellt in Artikel 14 folgende Anforderungen an eine Unterschrift:

1. *Die Unterschrift ist eigenhändig zu schreiben.*
2. *Eine Nachbildung der eigenhändigen Schrift auf mechanischem Weg wird nur da als genügend anerkannt, wo deren Gebrauch im Verkehr üblich ist, insbesondere wo es sich um die Unterschrift auf Wertpapiere handelt, die in grosser Zahl ausgegeben werden.*

¹So wird z. B. aus Kanada rechtsradikales Schriftengut übers Internet verbreitet, ohne dass andere Länder einschreiten können.

²Das amerikanische Gesetz verbietet die Ausfuhr gewisser kryptographischer Verschlüsselungsalgorithmen wie sie z. B. im Programm PGP verwendet werden.

Bisher schliesst diese Gesetzgebung die Verwendung digitaler Unterschriften aus. Da die digitale Unterschrift alle Anforderungen an eine Unterschrift erfüllt, wäre sie ein geeignetes Mittel zur Identifizierung und Anerkennung auf dem Internet. Eine gesetzliche Regelung lässt aber zumindestens in der Schweiz noch auf sich warten. Bei verschiedenen Bundesämtern, wie etwa dem Bakom, dem Bundesamt für Kommunikation, laufen zur Zeit die Arbeiten für die Ausgestaltung der Rahmenbedingungen.³

Kreditkarten

Die Idee der Verwendung von Kreditkarten“ über Distanzen hinweg“ stammt ursprünglich aus dem Teleshopping-Bereich und dem Versandhandel. Trotzdem fehlt vielen Kunden das Vertrauen bei der Verwendung ihrer Kreditkarte im Internet. Die rechtlichen Grundlagen sind zwar dieselben, allerdings sind sie noch ziemlich unklar. Es liegen in der Schweiz keine Bundesgerichtsurteile vor, und auch aus dem Ausland sind keine Urteile bekannt geworden. Es scheint, als wollen die Kreditkartenfirmen in diesem Bereich keine gesetzlichen Regelungen. Dazu passt, dass trotz mehrfachem Nachfragen bei VISA und MasterCard keine Antworten zu diesem Themenbereich zu erhalten waren.

Rosenthal⁴ ist der Meinung, dass “für missbräuchliche Verwendung eines Kartenkontos, der Karteninhaber nur haftet, wenn ihm die Karte selbst abhanden gekommen ist”. Für Rückgriffe auf den Karteninhaber muss die Karte selbst, und nicht nur Angaben darauf, einem Täter in die Hände gefallen sein. Das Risiko bei der Datenübermittlung ist für den Kunden nicht höher, als bei der normalen Verwendung der Kreditkarte, auch da werden die Daten auf der Karte von Dritten gesichtet.

Rosenthal ist weiter der Ansicht, “dass es an den Kreditkartengesellschaften liege, sichere Identifizierungsmethoden [und auch Übermittlungsverfahren] für Händler einzuführen”. Dies erklärt auch die grossen finanziellen Beteiligungen der Kreditkartenfirmen am SET-Projekt, siehe dazu Kapitel 4.3.

Digitales Geld

Die Herausgabe von digitalem Geld ist bis heute nicht dem Bankengesetz (BaG) unterstellt.⁵ Theoretisch ist also jedermann berechtigt, digitales Geld herauszugeben. In der Praxis stellt sich vielmehr das Problem, dass der Gläubiger die digitale Geldeinheit auch als Zahlungsmittel akzeptiert. Für einen sinnvollen Einsatz im grossen Rahmen sind Einschränkungen zur Herausgabe von digitalem Geld ebenso notwendig wie bei normalem Geld. Die heutige Situation gleicht jener im 18. Jh. in Schottland. Sowohl die Bank of Scotland als auch die von den Engländern gegründete Royal Bank gaben eigenes Geld aus und versuchten, die andere Bank aus dem Wettbewerb zu werfen. Bis etwa 1760 kamen weitere Banken hinzu, die ebenfalls alle ihre eigene Währung herausgaben. Als 1771 alle schottischen Banken die Noten der anderen Banken zum Nennwert akzeptierten, stabilisierte sich das schottische Bankensystem.

In den nächsten Jahren ist auf dem Gebiet des digitalen Geldes nicht mit gesetzlichen Vorschriften zu rechnen. Inzwischen müssen die Herausgeber (Banken, Kreditkartenunternehmen oder andere grosse Unternehmen wie Microsoft, AT&T, etc.) selber Händler finden, die ihr digitales Geld akzeptieren und so

³Handelszeitung Nr. 15 vom 8. April 1998, “Überregulierung soll vermieden werden”, S. 5

⁴D. Rosenthal, “Projekt Internet”, Verlag Finanz und Wirtschaft, Zürich 1997, S. 310ff.

⁵D. Kunz, Seminar Informatik und Recht “Rechtsfragen der Applikation Ecash”, Universität Zürich 1997, S. 28

dem Konsumenten auch Gelegenheit bieten, das erworbene, digitale Geld auszugeben.

Für Kunden ergibt sich das Problem des Vertrauens in den Herausgeber von digitalem Geld, falls es sich nicht um Banken handelt. Firmen, die nicht dem BaG unterstehen, können beispielsweise von der SNB, der Schweizerischen Nationalbank, nicht zur Haltung von Mindestreserven und einer gewissen minimalen Liquidität gezwungen werden und werden von dieser auch nicht revidiert. Im Falle eines Konkurses ist der Konsument somit wesentlich schlechter geschützt.

3.2 Kosten und Nutzen des Zahlungsverkehrs

Aus gesamtwirtschaftlicher Sicht sind die Kosten, die der ZV verursacht, beträchtlich. Lehmann⁶ schätzt die Kosten auf rund 1% des Bruttosozialproduktes. Für die Post betragen beispielsweise die Kosten 1990 für den Postzahlungsverkehr 1042,8 Mio. Franken. Wie oben erläutert, gehört die Schweiz zu den Bargeldländern. Dabei werden allerdings etwa 11 Mrd. Franken, bei einer Gesamtmenge von 32 Mrd. Franken⁷, von der SNB nur zur Verfügung gestellt, damit Kunden bei der Post pro Jahr 265 Mio. Einzahlungsscheine gegen Bargeld in Auftrag geben können.

Im folgenden wird auf die entstehenden Kosten und Nutzen, für die an einer Zahlungstransaktion beteiligten Parteien, getrennt eingegangen. Es werden zuerst die Kosten analysiert, die bei der Verwendung herkömmlicher ZV-Produkte entstehen. Danach werden zum Vergleich jene Kosten aufgezeigt, die beim Gebrauch von Internet-Zahlungsmitteln entstehen.

3.2.1 Kosten und Nutzen herkömmlicher ZV-Produkte

Die Zahlen und Beispiele dieses Kapitels sind hauptsächlich dem Buch von Schaufelberger entnommen.⁸

Kosten für Finanzinstitute

Die erste Kostenquelle für die Finanzinstitute beim ZV mittels Plastikgeld ist die Aquirierung von genügend Karteninhabern und Vertragshändlern. Der Teufelskreis besteht darin, dass Kunden nur Karten wollen, die sie bei genügend vielen Händlern benutzen können, und vice versa. Daneben müssen Kartenkonti eröffnet, Karten produziert, personalisiert und den Inhaber zugeschickt werden. Weiter entstehen Kosten aus der Kreditwürdigkeitsprüfung bei Kreditkartenkunden. Alle diese Kosten zusammen werden als *Kosten für den Neukartenservice* bezeichnet. Karten haben aus Sicherheitsgründen im allgemeinen eine Dauer von maximal zwei Jahren. Nach Ablauf dieser Frist, oder bei vorzeitigem Kartenverlust, entstehen *Erneuerungskosten*.

Weiter entstehen Kosten bei der *Verwendung* von Karten. Eine Kreditkartentransaktion kostet in den USA heute etwa US\$ 1.20, in Australien ungefähr \$A 2.10.⁹ Diese Zahlen variieren von Land zu Land.

Aber auch durch andere ZV-Produkte wie Schecks, Barein- und auszahlungen, Überweisungen mittels grünem Einzahlungsschein und Zahlungsaufträgen entstehen hohe Kosten. All jene Produkte, welche eine vollelektronische Verarbeitung verhindern, sind besonders teuer. So kostet die Verarbeitung eines Einzahlungsschein im Durchschnitt deutlich mehr als einen Franken. Ein Schalterkontakt eines Bankkunden – normalerweise mit einer Barabhebung verbunden – verursacht Kosten von über 25 Franken. Trotzdem sind beide Dienstleistungen bisher für den Kunden gratis.

Kosten und Nutzen für den Handel

ZV bedeutet für jeden Händler Kosten irgendwelcher Art. Bei der Verwendung von Bargeld entstehen Kosten durch zu treffende Sicherheitsmassnahmen und

⁶G. D. Lehmann, "Zahlungsverkehr der Banken", Verlag des Schweizerischen kaufmännischen Verbandes, Zürich 1992, S. 19

⁷siehe Bilanz 1997 der SNB

⁸K. Schaufelberger, "Kartengestützte Zahlungssysteme", Peter Lang AG, 1995, S. 94ff.

⁹A. Furche und G. Wrightson, "Computer Money", dpunkt, 1996, S. 17

durch die manuelle Abrechnung. Bei Bezahlung mittels grünem Einzahlungsschein bei der Post hat der Empfänger, also der Verkäufer, eine Taxe zu bezahlen. Bis zu einem Betrag von 50 Franken beträgt die Taxe 1.20 Franken und wächst dann stetig mit der Grösse des einbezahlten Betrages.¹⁰

Entschliesst sich ein Händler, seinen Kunden ein herkömmliches, elektronisches ZV-Mittel (nicht über Internet) anzubieten und auch seinen ZV teilweise elektronisch abzuwickeln, so fallen für ihn ebenfalls diverse Kosten an. Die grösste Ausgabenkomponente stellt für Vertragshändler von Kreditkartenfirmen die Kommissionsgebühr dar, deren Durchschnitt etwa bei 3% des Umsatzes liegt. Es ist den Händlern vertraglich untersagt, eine Preisdifferenzierung zwischen mit Kreditkarten und Bargeld bezahlten Gütern zu machen.

Als Anschaffungskosten fallen einmal Investitionskosten für Hard- und Software an. Die Kosten steigen mit der Anzahl Kartenarten (ec-direct, Postomat-Plus, VISA, Eurocard, etc.), Einzel- oder Mehrplatzlösungen und der Bandbreite der Datenleitung (Telefon, ISDN-Anschluss, etc.). Neben den reinen Anschaffungskosten fallen weiter auch Installationskosten, z. B. für Telefonleitungen, an.

Am Beispiel einer EFTPOS-Einrichtung einer grossen Schweizer Detailhandelsunternehmung sind in Abbildung 3.1 die Kosten einer solchen Lösung aufgelistet.¹¹ Zusätzlich zu den Investitionskosten sind Wartungskosten von Fr. 14,400.– pro Jahr zu zählen.

Kundenmodule		
25 Kundenmodule	à 3,660.–	91,500.–
25 Softwarelizenzen Kundenmodul	à 300.–	7,500.–
25 Softwarelizenzen KM-Klasse	à 120.–	3,000.–
Zubehör Kundenmodule		
25 DOV-Modems	à 920.–	23,000.–
25 Interfacekabel	à 160.–	4,000.–
Konzentrator		
1 Konzentrador K93		13,500.–
1 Drucker		2,500.–
1 Softwarelizenz K93		10,000.–
Zubehör Konzentrador		
2 zentrale Modem DOV	à 1,100.–	2,200.–
2 Modem Kabel	à 150.–	300.–
Diverses		
Installations- und Projektierungskosten		19,000.–
Umbau Telefonanlage		
Umbauarbeiten POS (35 Anschlüsse)		18,500.–
Total		195,000.–

Abbildung 3.1: Kosten für eine EFTPOS-Mehrplatzlösung

Für ZV-Produkte bei denen eine Verbindungserstellung zur Bank notwendig ist (EFTPOS-Produkte) kommen weiter die Kommunikationskosten dazu. Schlussendlich sind noch Schulungskosten für das Personal und, bei Kreditkarten, entgangene Zinserträge zu erwähnen, die ebenfalls zu Lasten des Verkäufers gehen.

¹⁰Vgl. "Tarifübersicht zum Postkonto", Post, gültig seit 1. Februar 1997.

¹¹Die Zahlen beruhen auf einer Offerte der Ascom Autelca, sind aber zum Schutz der Identität der betreffenden Unternehmung leicht geändert.

Demgegenüber stehen Kosteneinsparungen durch den Gebrauch von Karten. Der entstehende Nutzen ist allerdings nicht so leicht quantifizierbar wie die Kosten. Zu erwähnen ist der sinkende Anteil von Bargeld und dem damit verbundenen, geringeren Risiko. Ein niedrigeres Risiko bedeutet eine Verminderung der Versicherungsprämie. Der Mehrumsatz dank kartengestützten Zahlungssystemen kann ebenfalls kaum quantifiziert werden. Man ist sich jedoch mehr oder weniger einig, dass ohne entsprechende Systeme – vor allem internationale – Kundschaft verloren ginge. Als letztes übernimmt der Kartenerausgeber – bei Einhaltung der entsprechenden Vorsichtsmassnahmen – die Zahlungsgarantie. Dadurch reduziert sich das Ausfall-Risiko gegenüber einem Kauf auf Rechnung für den Händler beträchtlich.

Kosten und Nutzen für die Kunden

Allgemein ist klar, dass die Kunden schlussendlich einen Teil der Kosten tragen, die dem Handel durch den ZV entstehen. Der Preisbildungsprozess dürfte aber durch andere Faktoren stärker beeinflusst werden als durch diese ZV-Kosten.¹² Neben den Transaktionskosten hat der Kunde teilweise für weitere Kosten aufzukommen. Während Debitkarten normalerweise gratis abgegeben werden oder eine Jahresgebühr von höchstens 20 Franken aufweisen, sind die Kosten für Kreditkarten wesentlich höher. Die Spanne der Jahresgebühren reicht von 50 Franken bis zu 300 Franken.

Auch für Zahlungsüberweisungen mit Zusatzdienstleistungen muss der Kunde zahlen. So verlangt die Post beispielsweise für Eilüberweisungen 16 Franken, für sofortige Gutschrift 8 Franken. Die Credit Suisse verlangt pro nicht codiertem Zahlungsauftrag 3 Franken.

Der quantifizierbare Nutzen für den Kunden liegt in günstigeren Wechselkursen beim Benützen der Karte im Ausland, sowie durch Zinsvorteile. Bei Debitkarten – als pay-now Zahlungsmittel verwendet – bleibt das Geld des Kunden länger auf seinem Konto, bei der Verwendung von Kreditkarten wird dem Karteninhaber zusätzlich ein Kredit gewährt.

Neben diesen quantifizierbaren Nutzen entstehen weitere qualitative Vorteile. So reduziert sich das Bargeldrisiko für den Inhaber von Debit- und Kreditkarten. Der Inhaber von internationalen Kreditkarten (Visa, MasterCard, American Express, etc.) muss im Ausland nicht verschiedene Währungen auf sich tragen. Viele Karten gewähren zudem Nebenleistungen wie Reiseunfallversicherung, Übernahme von Bergungs-, Such- und Rückflugkosten oder Flugunfallversicherung.

3.2.2 Kosten im Internet

Bei der Analyse der Kosten muss zwischen Initialkosten und den laufenden Kosten, welche wiederum aus fixen und variablen Anteilen bestehen, unterschieden werden. In diesem Kapitel werden die Kosten nur allgemein betrachtet, eine detailliertere Aufstellung wird in Kapitel 4 für die vorgestellten Produkte gegeben.

Initialkosten

Der ZV via Internet fordert im allgemeinen den Einsatz spezieller Software, in seltenen Fällen auch spezialisierter Hardware. Die Software wird dem Kunden

¹²P. Frazer, "Plastic and Electronic Money: New Paymentsystems and their Implications", Woodhead-Faulkner, Cambridge 1985, S. 31

meist frei zur Verfügung gestellt, z. B. Client-Software bei ecash, oder bereits standardmässig zum System mitgeliefert, z. B. Internet-Browser mit SSL Unterstützung.

Auf Händlerseite sind grössere Initialinvestitionen nötig. Die Aufschlüsselung ist allerdings schwierig: Die Server-Software wird im allgemeinen als Gesamtpaket, z. B. Netscape Commerce Server mit SSL, verkauft, welche die Funktionalität für den gesamten E-Commerce enthält. Ebenso wird der Server häufig bei einem Internet Service Provider (ISP) aufgestellt, welcher für seine Dienste einen fixen Betrag, unabhängig von der Art, der auf dem Server angebotenen Services, verlangt.

Im Vergleich zu den Kosten des herkömmlichen ZV (siehe als Beispiel Abbildung 3.1) sind die Initialkosten beinahe verschwindend klein.

Fixe Kosten im Betrieb

Zu den fixen Kosten im Betrieb, d. h. den regelmässig wiederkehrenden Kosten, welche nicht vom Zahlungsvolumen abhängig sind, gehören Lizenzgebühren für Softwarebenutzung, Abgaben für Erneuerungen von Zertifikaten³ und auch fixe Anschlussgebühren, welche nicht vom Kommunikationsvolumen abhängig sind. Das Kommunikationsvolumen für den ZV ist im Vergleich zur restlichen Kommunikation (z. B. Darstellung von WWW-Seiten) verschwindend klein.

Variable Kosten im Betrieb

Der ZV über das Internet verursacht verschiedene variable Kosten. Allen Produkten gemeinsam sind Kosten für die Kommunikation, sofern diese volumenabhängig verrechnet werden. Dies ist je nach Internet Service Provider unterschiedlich. Diese Kommunikationskosten sind allerdings normalerweise so klein, dass sie höchstens bei Mikrozahlungen ins Gewicht fallen.

Bei kreditkartenbasierten Lösungen (wie SSL oder SET) entstehen die regulären Transaktionskosten¹⁴, welche identisch sind zu denjenigen im herkömmlichen ZV. Sparpotential besteht in erster Linie im einfacheren und zuverlässigeren Erfassen der Kreditkartendaten sowie in der Möglichkeit, diese Daten automatisch in ein Buchhaltungssystem zu übertragen.

Debitorenverluste

Ein wichtiges Argument für die Einführung von Internetzahlungsmitteln sind die Debitorenverluste. Diese sind bei kleinen Rechnungsbeträgen, bei denen sich eine Betreuung nicht lohnt, erheblich und können durch den Einsatz von Kreditkarten oder in noch grösserem Umfang durch ecash oder ähnliche Systeme massiv reduziert werden. Im Gegensatz zur Vorauszahlung per Scheck oder Überweisung ergeben sich so keine Verzögerungen der Zahlung.

3.2.3 Kosten als Erfolgsfaktoren

Für Händler, die schon über ein herkömmliches ZV-System verfügen, stellt die Anschaffung eines neuen Systems in erster Linie einen Kostenfaktor dar. Der Händler muss erst in ein neues System investieren und seinen Kunden dessen Vorteile kommunizieren, bevor er, hauptsächlich bei den Debitorenverlusten,

¹³<http://www.verisign.com>

¹⁴Typischerweise sind dies 2 bis 4% vom Umsatz.

seine Investitionskosten wettmachen kann. Sobald die Transaktionsdaten automatisch in ein Buchhaltungssystem übertragen werden, können weitere Kosten gespart werden.

Für den Kunden sind die Kosten des ZV nicht transparent. Die einzige Ausnahme bilden Einkäufe im Ausland, welche nicht über Kreditkarten abgewickelt werden. Hier können die Kosten vom Kunden wahrgenommen werden. Ansonsten liegt es an den Händlern, den Kunden die Preisvorteile von elektronischen Systemen zu kommunizieren, beispielsweise durch Rabatte, Prämien auf den Umsatz oder andere Verkaufsförderungsmaßnahmen.

Aus finanzieller Sicht am meisten Interesse an einem Umstieg auf elektronische ZV-Instrumente auf dem Internet haben auf der Kostenseite die Finanzinstitute, d. h. Kreditkartenfirmen und Banken, sowie die Post. Banken und die Post können einerseits die Kosten senken, welche durch den ZV entstehen. Finanzinstitute können andererseits Betrugsrisiken und -möglichkeiten mittels technischer Verfahren wie SSL und SET (siehe Kapitel 4) senken.

3.3 Sicherheit und Vertrauen

Je genauer ein elektronisches Produkt die bekannten ZV-Instrumente abbildet, desto höher dürfte auch die Kundenakzeptanz und das dem Produkt entgegengebrachte Vertrauen sein. Die Anlernzeit an ein solches Produkt wird kleiner und ein Kunde kann schneller produktiv und zeitsparend damit arbeiten. Laut einer Umfrage sind Käufer von entsprechenden Softwareprodukten denn auch bereit, „*einfach zu gebrauchende* Homebanking- und Handelsprodukte zu benützen, falls diese Zeit und Geld sparen“¹⁵.

Wie muss ein ZV-Produkt für das Internet beschaffen sein, damit es eine hohe Kundenakzeptanz aufweist? Der Bericht geht in der Folge davon aus, dass der Käufer auf dem Internet jene ZV-Instrumente vorfinden will, die er bisher auch im Alltag gebraucht hat. Das heisst also, dass ein schweizerischer Kunde hauptsächlich mit digitalem Geld und Kreditkarten bezahlen will, während sein amerikanisches Pendant die elektronische Abbildung eines Schecks bevorzugen dürfte.

Die Unterschiede in der Wahl der ZV-Instrumente sind weltweit stark verwurzelt und Änderungen im Verhaltensmuster nur schwer durchzusetzen. Ebenfalls hinderlich sind dabei die Abhängigkeiten der am ZV beteiligten Partner.¹⁶ Obwohl auch die Schlussfolgerung zulässig wäre, dass, wenn ein Käufer schon auf ein elektronisches Medium umsteigt um seinen ZV zu erledigen, dass er dann gleich auch sein(e) Instrument(e) wechseln könnte, so erscheint dies aus den oben genannten Gründen für eine breitere Bevölkerungsschicht eher unwahrscheinlich.

Eine Umfrage der Softwarehersteller zu diesem Thema könnte sicher einige Zweifel klären und helfen, Fehlinvestitionen zu vermeiden, bzw. neue Systeme zu konzipieren und zu fördern. Allgemein scheinen gewisse Zufälligkeiten in der Entstehung von digitalen Zahlungsmitteln recht häufig. So kann man sich etwa die Frage stellen, weshalb DigiCash's ecash als pre-paid Zahlungsmittel und nicht beispielsweise als pay-now Produkt konzipiert wurde.

Der Begriff der Anonymität darf im Zusammenhang mit dem Kapitel "Sicherheit und Vertrauen" ebenfalls nicht fehlen. Vielen Käufern fehlt das Vertrauen in die Besitzer von Datensammlungen, sei dies in eine Institution wie Payserv, welche in der Schweiz das SIC und die Bancomaten betreibt, oder in Handelsbetriebe wie beispielsweise die Migros mit ihrer Cumuluskarte.

Im herkömmlichen ZV besteht für den Konsumenten die Möglichkeit, durch Barzahlung anonym zu bleiben. Gleichzeitig hat der Staat, etwa bei Erpressung, über die Seriennummern der Geldscheine gewisse Kontrollmöglichkeiten. Bezüglich Anonymität sind damit sowohl Kunden als auch der Staat mit der Verwendung von Bargeld zufriedenstellend bedient.

Daraus resultieren auch für Internet-Zahlungsprodukte gewisse Anforderungen bezüglich Anonymität. Obwohl bei herkömmlichen Produkten oft gar nicht wahrgenommen wird, dass die Anonymität nicht vollständig gewährleistet ist, achtet der Konsument bei neuen Produkten verstärkt darauf und lehnt Produkte ohne genügende Anonymität ab. Auf dem Markt werden sich längerfristig nur Produkte durchsetzen, welche genügend Anonymität aufweisen, und dies ihren potentiellen Kunden auch kommunizieren können.

Dass sich der ZV via Internet nur durchsetzen wird, falls der Kunde dem E-Commerce als Ganzes vertraut, ist offensichtlich und sei hier nur am Rande

¹⁵D. C. Lynch, "digital money", John Wiley & Sons, Inc., 1996, S. 123

¹⁶G. D. Lehmann, "Zahlungsverkehr der Banken, Verlag des Schweizerischen Kaufmännischen Verbandes, 1992, S. 15

erwähnt. Dass Kundenprofile beim Einkauf übers Netz vom Verkäufer besser erfasst werden können, ist eine Tatsache, die nicht umgangen werden kann. Der Kunde hat mit einem ihm persönlich angepassten und auf ihn abgestimmten Marketing zu leben (Direkt-Marketing¹⁷).

¹⁷A. Seiler, "Marketing", Orell Füssli, Zürich 1992, S. 339

3.4 Zeit

“Zeit ist Geld.” Diese Weisheit trifft auch im ZV zu. Eine Zahlungstransaktion soll sowohl für den Kunden als auch für den Verkäufer möglichst schnell abgewickelt werden, beide Parteien sind daran interessiert, Zeit und Geld, wenn nicht zu sparen, dann nicht zu verlieren.

Im herkömmlichen ZV versuchen einerseits die Banken, Transaktionen von Bargeld zwischen ihnen und ihren Kunden von den Schaltern weg, so weit wie möglich an ATM's zu verlagern, um Raumkosten zu sparen und das Personal von zeitaufwendigen Ein- und Auszahlungen zu befreien. Im Laden wird andererseits der Einsatz von elektronischen Zahlungsmitteln gefördert, um das nicht maschinell weiterzuverarbeitende Bargeld und Schecks durch EFTPOS-Terminals und Kreditkarten zu ersetzen. In beiden Fällen können personelle und finanzielle Ressourcen freigesetzt werden.

Auch für den Kunden bieten sich immer neue ZV-Produkte an, die den Zeitaufwand für Zahlungen verkleinern. Die Kunden wollen beispielsweise nicht bei jedem grösseren Kauf zuerst den nächsten Bancomaten aufsuchen, Geld abheben und danach im Geschäft ihre Transaktion beenden, sondern im Geschäft über ein EFTPOS-Terminal die gesamte Transaktion abwickeln. Auch die Einzahlungen am Postschalter können Zeit und Nerven kosten. Sie werden aber u. a. aus Kostengründen – die Banken verlangen Gebühren für nichtcodierte Zahlungsaufträge – trotzdem in Kauf genommen.

Beim Einkauf übers Internet bevorzugt der Kunde aus Zeitersparnisgründen die schnellstmögliche und bequemste Zahlungsart, wie er dies auch bisher versuchte. Es ist unsinnig, wenn Kunden übers Internet bestellen können, danach aber mit einem Einzahlungsschein zur nächsten Post geschickt werden, um in einer Schlange zu warten, bis sie bezahlen können. Trotzdem existieren gerade in der Schweiz noch unzählige Internetseiten, die dem Kunden genau dieses Verfahren aufzwingen. Wieviel einfacher kann hier eine Zahlung mittels Kreditkarte oder digitalem Geld erfolgen! Kann der Kunde seine Zahlungen erst noch direkt in seine eigene Buchhaltung einfließen lassen, etwa mittels Programmen wie Quicken¹⁸, so hat er effektiv Zeit eingespart.

¹⁸D. C. Lynch, “digital money”, John Wiley & Sons, Inc., 1996, S. 4

3.5 Qualität und Flexibilität

Flexibilität ist für den Kunden bezüglich Zeitpunkt, Ort und Art des Zahlens von Bedeutung. Je mehr Flexibilität ein Produkt in diesen Bereichen anbieten kann, desto höher sind seine Marktchancen. Zur Art des Zahlens gehört, dass der Kunde wählen kann, ob er den Verkäufer direkt bezahlen will oder auf Kredit einkaufen will. Weiter gehört die Möglichkeit, eine Transaktion zu widerrufen, dazu. Kauft ein Kunde in einem Geschäft ein, kann er den gekauften Artikel zurückzubringen und erhält sein Geld in Bar zurück, dies selbst dann, wenn er mit EFTPOS-Systemen oder Kreditkarte bezahlt hat. Dies wird bei virtuellen Einkäufen schwieriger.

Die Kosten, die bei einer Zahlungstransaktion entstehen, schränken die Verwendung von gewissen Produkten für bestimmte Beträge ein. So macht es keinen Sinn, für Beträge unter ein paar Franken mit Kreditkarte zu bezahlen. Die dem Händler entstehenden Kosten wären höher als die Einnahmen durch den Verkauf. Das gleiche gilt auch für Transaktionen im Internet. Es wird zwischen *Micro- (kleine Beträge)* und *Makro-Payment (grössere Beträge)* unterschieden. Quantitative Grenzen hängen von den spezifischen Produkten ab.

Ein eher technisches Problem stellt die Inkompatibilität von Browsern dar. Die ZV-Systeme müssen so konzipiert sein, dass sie auf den wichtigsten verfügbaren Browsern laufen (zumindestens mit dem Netscape-Browser und dem Explorer von Microsoft). Nur browser- und plattformübergreifende Softwareprodukte sind genügend flexibel, um auf dem Markt eine Chance zu haben.

Zwei Dinge muss eine ZV-Software erfüllen, damit sie einen gewissen Qualitätsstandard erreicht: Zuverlässigkeit und Einfachheit im Gebrauch. Beide Punkte betreffen sowohl die Kunden- als auch die Händlersicht. Der Kunde erwartet ein Produkt, das er ohne Anleitung intuitiv bedienen kann. So vermeiden Teilnehmer an einem Test den Gebrauch von digitalen Signaturen, weil sie diese als unangenehm empfanden als eine Unterschrift von Hand.¹⁹ Den Händlern sollen die ZV-Produkte die Arbeit erleichtern und Kosten sparen helfen, sowie neue Kundenkategorien erschliessen.

Die Zuverlässigkeit muss ebenfalls beidseitig gewährt werden. Der Kunde will sicher sein, dass einerseits seine Zahlung erfolgt ist, andererseits will er nur für Dinge bezahlen, die er auch bestellt hat. Betrugsmöglichkeiten sollen soweit als möglich ausgeschlossen werden. Dem Verkäufer liegt daran, das erhaltene Geld oder die Kreditkartennummer bei einer Bank vorweisen zu können und dafür ohne Probleme Geld zu bekommen. Insbesondere bei Offline-Systemen kann für den Händler das Problem des Double-Spendings auftreten. Händler werden also nur für den Einsatz von ZV-Produkten via Internet zu gewinnen sein, wenn Banken, Kreditkartenfirmen oder andere Herausgeber entsprechender Produkten faire und für die Händler nicht nachteilige Verträge anbieten.

¹⁹D. Whinnett, "End User Acceptance of Security Technology for Electronic Commerce", Universität Freiburg, Deutschland 1996

Kapitel 4

Angebote Produkte

4.1 First Virtual

Die Firma First Virtual Inc.¹ wurde 1994 gegründet und kann als eine der ersten wirklich virtuellen Firmen bezeichnet werden. Die Firmenleitung ist von San Francisco bis Washington, DC verteilt. Treffen werden regelmässig über Telefonkonferenzen und e-mail abgehalten. Ihr Produkt "First Virtual" wurde als eines der ersten Modelle für den Internet-ZV angeboten. Das System basiert auf e-mail und der Verwendung von Kreditkarten und zeigt eine relativ einfache Möglichkeit des ZV im Internet auf.

4.1.1 Funktionsweise des Systems

Damit ein Kunde über First Virtual bezahlen kann, muss er bei der Firma eine persönliche Identifikationsnummer (VirtualPIN) beantragen. Will der Kunde einen Kauf tätigen, ergänzt er das Bestellformular des Verkäufers mit den gewünschten Produkten und seiner VirtualPIN und sendet das Formular via e-mail an den Verkäufer. Dieser bearbeitet die Bestellung und sendet die Rechnung mit seiner eigenen VirtualPIN und derjenigen des Kunden an First Virtual, wiederum über e-mail. First Virtual sendet dem Käufer eine Belastungsanzeige, die dieser bestätigen, widerrufen oder als Betrugsversuch melden kann. Bestätigt der Kunde die Transaktion, wird der Verkäufer benachrichtigt – der ab dann innert 24 Stunden liefern muss – und die Kreditkarte des Kunden zugunsten von First Virtual belastet. Über das amerikanische Clearingsystem, das United States Automated Clearing House System (ACH) wird dem Händler den ihm zustehenden Betrag ausbezahlt. Bei Widerruf der Zahlung sollte der Grund dem Verkäufer direkt begründet werden, bei wiederholtem Widerruf *nach* Erhalt der Ware kann ein Kunde ausgeschlossen werden.

Der Hauptteil der sensitiven Aktionen der Zahlungstransaktion geschieht bei First Virtual ausserhalb des Internets, sie werden über das ACH zwischen First Virtual, den Banken und den Kreditkartenfirmen abgewickelt. Das Internet dient technisch gesehen ausschliesslich der Bestellung und Bestätigung. Die Kosten für die Händler bestehen aus einer einmaligen Application-Gebühr von US\$ 645 für Express Händler, bzw. von US\$ 390 für Pioneer Händler. Der Unterschied zwischen den 2 Varianten besteht in der Zeit die verstreicht, bis der Händler sein Geld erhält. Bei Express Händlern sind dies höchstens 21 Tage, bei Pioneer Händlern bis zu 108 Tage. Weiter ist eine Jahresgebühr von

¹<http://www.firstvirtual.com>

US\$ 450 für Express Händler, bzw. US\$ 200, zu bezahlen. Die Transaktionskosten belaufen sich auf 2% des Umsatzes plus 29 Cents pro Transaktion. Für die kumulierten Überweisungen auf das Konto des Händlers wird nochmals eine Gebühr von US\$ 1 verlangt.

4.1.2 Vor- und Nachteile

Durch die Abwicklung der eigentlichen Finanztransaktion über das ACH-Netz entstehen beim System keine Probleme mit der Unsicherheit von Internet-Transaktionen. Aus der Sicht des Kunden wird die gesamte Zahlungstransaktion bequem und einfach übers Internet abgewickelt, was hinter den Kulissen läuft, muss ihn nicht interessieren. Selbst bei Missbräuchen kann der Kunde diese melden und muss nicht für den entstandenen Schaden aufkommen. Falls ein Händler vor Erhalt einer Bestätigung liefert, trägt er im Betrugsfall den Verlust, andernfalls wird der Betrug aufgedeckt, bevor jemand zu Schaden gekommen ist.

Die Anonymität des Kunden bleibt gegenüber dem Händler nur beim Bezahlen von übers Internet gelieferten Informationen gewahrt, da er in diesem Fall nur seine VirtualPIN liefert, nicht aber seinen Namen. Bei Hauslieferungen muss der Händler die Lieferadresse kennen. Gegenüber First Virtual besteht kein Anonymitätsschutz, die Firma behält sich im Vertrag sogar vor, sämtliche Transaktionen in ihrer Datenbank zu speichern.

Vorteile für den Händler liegen in den tiefen Anschaffungskosten. Diese sind weit unter denjenigen für herkömmliche Zahlungssysteme. Im Betrieb werden die Kosten jedoch relativ hoch, allerdings immer noch tiefer als bei herkömmlichen ZV-Produkten. Dadurch ist das System nicht für Beträge im Cent-, bzw. Rappenbereich geeignet, da sonst die Transaktionskosten die Einnahmen übertreffen. Weiter muss der Händler nicht mit Debitorenverlusten rechnen und kann seinen Debitorenumschlag im voraus relativ genau berechnen, was das Cashmanagement vereinfacht. Ausserdem sind die gesendeten e-mails alle in einer standardisierten Form, sie können also digital weiterverarbeitet werden.

4.1.3 Referenzen

First Virtual war, wie schon erwähnt, eines der ersten Produkte für Internet-ZV, das auf den Markt kam. Es hat vor allem in den USA grosse Verbreitung gefunden. Beispiele sind PenComputing² und Internic³.

²<http://www.pencomputing.com>

³<http://www.internic.com>

4.2 SSL

Secure Sockets Layer (SSL) definiert ein Protokoll, welches geheime, authentische Kanäle über das Internet ermöglicht. SSL wird heute von den verbreiteten Browsern (Microsoft Internet Explorer und Netscape Navigator) unterstützt. SSL ist ein allgemeines Protokoll, welches nicht auf den ZV beschränkt ist, sondern generell eine sichere Kommunikation über Internet ermöglicht unter Verwendung von beliebigen kryptographischen Algorithmen. Durch die einfache Verfügbarkeit ist SSL heute die am weitesten verbreitete Möglichkeit, um einen sicheren ZV über das Internet zu implementieren: Die Kreditkartennummer wird hierbei über den gesicherten Kanal zum Händler übertragen. SSL ermöglicht theoretisch eine gegenseitige Authentifikation. In der Praxis ist nur eine Authentifikation des Diensteanbieters gegenüber dem Kunden implementiert, sonst wäre der Kunde gezwungen, sich ebenfalls ein eigenes Zertifikat zu kaufen.

4.2.1 Kosten

Bei der Verwendung von SSL entstehen neben den Verbindungskosten für den Kunden keine zusätzlichen Kosten. Für den Verkäufer entstehen die üblichen Kosten für Kreditkartentransaktionen.

Zertifizierte Schlüssel sind zwischen US\$ 349 (Secure Server ID) und US\$ 995 (EDI, Open Financial Exchange) pro Jahr bei VeriSign⁴ erhältlich.

4.2.2 Vor- und Nachteile

SSL ist ein einfach zu implementierendes Protokoll, welches eine enorme Verbreitung genießt. SSL ist deshalb heute meist erste Wahl, um sichere Transaktionen über das Internet zu ermöglichen.

SSL bietet nur eine Authentifizierung der Partner sowie einen sicheren Kanal. Weitergehende Sicherheit ist nur durch zusätzliche Protokolle (und damit zusätzlicher Software) möglich.

4.2.3 Referenzen

SSL wird an vielen Orten eingesetzt. Ein bekanntes Beispiel ist die Amazon-Buchhandlung⁵. Auch in der Schweiz wird SSL eingesetzt, z. B. im Zahlungssystem der Reimer AG⁶, siehe Kapitel 5.2.1.

⁴<http://www.verisign.com>

⁵<http://www.amazon.com>

⁶<http://www.reimer.ch>

4.3 SET

Secure Electronic Transaction (SET)⁷ beschreibt ein Protokoll zur sicheren Abwicklung von Kreditkartenzahlungen über offene Netze (Internet). SET bietet folgende Dienste:

- **Geheimhaltung der Daten** Um den Missbrauch von Kreditkarten (automatisiertes Suchen von Kreditkartennummern) zu reduzieren, werden bei SET alle Daten verschlüsselt übermittelt.
- **Integrität der Daten** SET gewährleistet mit Hilfe von digitalen Unterschriften, dass keine veränderte Meldung (Übertragungsfehler oder Betrugsversuch) vom Empfänger akzeptiert wird.
- **Authentifikation des Kunden** Ein Kunde authentifiziert sich gegenüber einem Händler als legaler Inhaber der Kreditkarte mittels digitaler Unterschrift sowie einem Zertifikat.
- **Authentifikation des Händlers** Ein Händler authentifiziert sich gegenüber dem Kunden als berechtigter Zahlungsempfänger mittels elektronischer Unterschrift sowie einem Händlerzertifikat.

SET wurde gemeinsam von VISA und MasterCard entwickelt. Technische Unterstützung bieten Firmen wie GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa und VeriSign. Dank der breiten, plattform-übergreifenden Unterstützung ist damit zu rechnen, dass SET in Zukunft eine der bedeutendsten Methoden für den ZV auf dem Internet darstellen wird. Wann genau SET jedoch wirklich relevant wird, ist schwer abzuschätzen: Die Kreditkartenfirmen propagieren SET schon seit einiger Zeit, konkrete Lösungen aber sind praktisch nicht erhältlich.

4.3.1 Implementation

SET ist noch nicht im allgemeinen Gebrauch, es existiert allerdings eine frei verfügbare Referenzimplementation von Terisa, basierend auf der RSA BSAFE⁸ Bibliothek.

BSAFE implementiert die folgenden kryptographischen Protokolle: Triple-DES, RC5, RSA, MD5 und SHA1. Die Zertifikate folgen dem X509 v3 Standard.⁹

4.3.2 Zertifikate

Verisign¹⁰ bietet für SET Zertifikate an.

4.3.3 Kosten

Mangels verfügbaren Implementationen sind die Kosten zurzeit schwer abschätzbar. Es ist anzunehmen, dass Initialkosten im Bereich von wenigen tausend Dollar für Software und Installation, jährliche Kosten von ein paar hundert bis tausend Dollar für die Erneuerung von Zertifikaten sowie die bei Kreditkarten üblichen Transaktionskosten von 2 bis 5% des Umsatzes anfallen werden.

⁷<http://www.set.ch>

⁸<http://www.rsa.com/rsa/products/bsafe>

⁹<http://www.software.ibm.com/commerce/payment/set-paper.html>

¹⁰<http://www.verisign.com>

4.3.4 Referenzen

In der Schweiz wird SET zurzeit von Europay¹¹ forciert. Am Pilotbetrieb werden maximal 40 Firmen und 400 Kunden teilnehmen. Die einzigen, bekannten Anbieter in der Schweiz sind der Pizzakurier SPK AG¹² sowie die Weinhandlung Martel AG¹³.

¹¹<http://www.europay.com>

¹²<http://www.pizzakurier.ch>

¹³<http://www.martel.ch>

4.4 ecash

ecash von DigiCash¹⁴ ist eine Implementation von anonymem, elektronischem Geld wie es im Abschnitt 2.2.2 beschrieben wird. DigiCash hat Ende 1994 einen ersten Testlauf für das System durchgeführt, seit 1995 ist das System kommerziell im Einsatz. Als Herausgeber von digitalem Geld tritt die Mark Twain Bank¹⁵ auf, andere Banken wie z. B. die Deutsche Bank führen zur Zeit einen Versuchsbetrieb durch.¹⁶ Kunden und Anbieter, welche das System nutzen wollen, müssen ein Konto bei der emittierenden Bank unterhalten.

4.4.1 Eigenschaften von ecash

ecash erfüllt folgende, an elektronisches Geld gestellte Anforderungen:

- **Fälschungssicherheit** wird durch elektronische Unterschriften gewährleistet.
- **Double-Spending** wird durch Seriennummern verhindert. Das System arbeitet mit nur einer Bank, die Überprüfung der Seriennummern gestaltet sich damit relativ einfach.
- **Anonymität** wird durch blindes Unterschreiben der Münze durch die Bank realisiert. Es existiert keine Möglichkeit, die Anonymität aufzuheben.

4.4.2 Software

Sowohl Kunde wie auch Anbieter müssen spezielle Software für den ZV verwenden. Auf Seite des Kunden ist dies eine Art elektronisches Portemonnaie, welches die Münzen speichert und Zahlungen auf Anforderung hin durchführt. Die Software ist verfügbar für alle Microsoft Windows Umgebungen sowie in einer einfacheren Form auch für UNIX Systeme.

Für die Implementation auf Anbieterseite existiert ein Toolkit, welches alle wichtigen Funktionen beinhaltet und sowohl auf UNIX wie auch auf Windows NT verfügbar ist. Dieses Toolkit wird über Standardinterfaces (z. B. cgi-bin) in den Web-Server eingebunden.

4.4.3 Kosten

ecash ist für den Kunden gratis: Die notwendige Software wird frei zur Verfügung gestellt, Transaktionskosten entstehen ihm keine.

Für den Anbieter entstehen Investitionskosten für die Lizenz und Installation der Software, zusätzlich wird pro Transaktion ca. 2% des Umsatzes oder Fr. 0.20 für kleine Beträge (bis ca. Fr. 30.-) verrechnet. Diese Beträge werden vermutlich noch sinken, insbesondere die Minimalgebühr von Fr. 0.20 ist derzeit für Micro-Payments zu hoch.

4.4.4 Referenzen

In der Schweiz führt seit Anfangs Juni die Swiss NetPay AG, siehe Kaptiel 5.2.3 einen Versuchsbetrieb mit ecash durch. International ist ecash ausser in

¹⁴<http://www.digicash.com>

¹⁵<http://www.marktwain.com>

¹⁶Die vollständige Liste der Anbieter ist unter <http://www.digicash.com> zu finden

den USA besonders in Finnland¹⁷ und Australien¹⁸ gut vertreten.

¹⁷<http://www.eunet.fi>

¹⁸<http://www.stgeorge.com.au>

4.5 Andere Projekte

Zur Zeit existiert eine Vielzahl von Produkten für den ZV via Internet. Die bisher vorgestellten Produkte repräsentieren die vorhandenen technischen Möglichkeiten, deswegen wird auf eine detailliertere Beschreibung weiterer Produkte verzichtet. Die Kategorie der scheckbasierten ZV-Produkte wird nicht genauer vorgestellt, da die Schweiz wie erwähnt kein Scheckland ist und diese Produkte somit auch keine grosse Verbreitung haben.

Nicht nur private Firmen sind an der Forschung und Entwicklung von Zahlungsmethoden übers Internet beteiligt. Auch staatliche Organisationen wurden mit dem Ziel ins Leben gerufen, länderübergreifende Systeme und technische Standards einzuführen. CAFE ("Conditional Access for Europe")¹⁹ entwickelte im Rahmen des EU-Forschungsprogrammes ESPRIT ein sicheres, anonymes Zahlungssystem für Offline-Zahlungen. Ein Konsortium mit Partnern aus Industrie, Finanz und Wissenschaft führt in Europa mit Unterstützung der EU das Projekt SEMPER²⁰ zur Entwicklung von Grundlagen für den sicheren elektronischen Handel durch.

Zum Abschluss des Kapitels werden weitere, bekannte Produkte tabellarisch dargestellt.

<i>Produktname</i>	<i>Vor- und Nachteile</i>	<i>Wichtigste Einsatzgebiete</i>
CyberCash http://www.cybercash.com	+Anonymität des Käufers bleibt gewahrt -Registrierung des Käufers und Verkäufers bei CyberCash notwendig	Alle Arten von Kreditkartenkäufen
NetBill http://www.netbill.com	+Bezahlung und einwandfreie Lieferung werden durch das System sichergestellt + Auch für sehr kleine Beträge einsetzbar -Nur für elektronisch gelieferte Produkte einsetzbar	Verkauf von elektronisch vertreibbarer Information und Software
Mondex Card http://www.mondex.com	+Elektronisches Geld auf Karte transportierbar +Mit günstigen Endgeräten fast überall einsetzbar -Noch fehlt Verbindung zum Internet	Bargeldersatz für Käufe in entsprechend ausgerüsteten Geschäften
Millicent http://www.millicent.digital.com	+Für sehr kleine Bereiche geeignet +Währungswechsel automatisch möglich -Erst in der Testphase	Für Mikropayment geeignet
NetCash http://www.teleport.com	+Wie Fremdwährung einsetzbar +Sehr sicher -Anonymität nicht voll gewährleistet	Couponsystem

¹⁹<http://www.informatik.uni-hildesheim.de/sirene/projects/cape>

²⁰<http://www.semper.org>

Kapitel 5

Internetzahlungsverkehr in der Schweiz

5.1 Auswertung der Umfrage

Um mehr über den aktuellen Umfang und die Art des ZV via Internet in der Schweiz herauszufinden, wurde bei 65 Firmen eine Umfrage durchgeführt, wovon 20 antworteten. Es wurde in der Umfrage unterschieden zwischen Firmen, welche bereits heute ihren ZV via Internet abwickeln (siehe Fragebogen im Anhang B.1) und solchen, welche nur die Bestellung über das Internet ermöglichen, für den ZV aber die herkömmlichen Wege beschreiten (siehe Fragebogen im Anhang B.2). Allerdings spielt dieser Unterschied für die Auswertung keine Rolle. Die Ergebnisse der Umfrage werden im folgenden, aufgeteilt nach Themen, erläutert.

5.1.1 Firmenprofil

In der Schweiz bieten heute in erster Linie kleine bis mittlere Handelsbetriebe Zahlungsmöglichkeiten via Internet an. Auffallend häufig werden multimediale Produkte angeboten (CDs, Software, Bücher), aber auch Nahrungsmittel und andere Konsumgüter können via Internet bestellt werden.

Diejenigen Firmen, welche Waren auf dem Internet anbieten, vertreiben bis auf wenige Ausnahmen das komplette Sortiment über diesen Kanal.

Grosse Unternehmen sind heute zwar auf dem Internet präsent, bieten aber nur Information an.

5.1.2 Allgemeine Einschätzung des Internets

Grundsätzlich kann festgehalten werden, dass sämtliche Firmen dem Internet gegenüber ausserordentlich positiv eingestellt sind. Das Interesse am neuen Medium ist vorhanden und entsprechend gut kennen sich die angefragten Firmen in diesen Gebieten aus. Nur einige kannten weniger als 2 der erwähnten Begriffe, was jeweils damit begründeten wurde, dass der komplette Internet-Auftritt von Dritten realisiert wurde.

Besonders interessant war die Frage nach den Chancen und Gefahren, welche die angefragten Firmen im Internet sehen. Hier war von Zurückhaltung bis Euphorie alles vertreten, die positiven Stimmen überwogen aber klar. Insbesondere kleine Firmen sehen grosse Chancen, sich mit bescheidenen Mitteln einen internationalen Markt zu erschliessen.

Die Gefahren werden allgemein als klein eingestuft. Eine gewisse Angst herrscht einzig vor Sicherheitslöchern. Eine Angst vor grösserer Konkurrenz ist nicht zu spüren.

Das sehr positive Echo muss natürlich kritisch hinterfragt werden. Eine Schwäche der Umfrage ist, dass nur Firmen befragt wurden, welche bereits auf dem Internet präsent sind. Eine weitere Ausdehnung der Umfrage würde vermutlich eine deutlich grössere Zahl von kritischen Stimmen ergeben.

5.1.3 Idee und Einführung

Die Idee für den Internet-Auftritt kommt in der überwiegenden Mehrheit von der Geschäftsleitung, nur in wenigen Fällen wurde die Marketing- oder EDV-Abteilung genannt. Entschieden wird ebenso deutlich in der Geschäftsleitung oder im Verwaltungsrat.

Bei der Realisierung des Auftrittes sind die Antworten breit gefächert. Externe Firmen werden etwa gleich häufig wie die eigene Informatik als Verantwortliche genannt. Auffallend ist, dass nur wenige Firmen auf externe Beratung verzichten. Internet-Consultants dürften daher in Zukunft eine wichtige Funktion einnehmen, wenn es darum geht, neue ZV-Produkte zu verbreiten.

Eine einheitliche Vorgehensweise bei der Einführung ist nicht zu erkennen, die Etappen des Projektes wurden recht unterschiedlich angegeben. Die Antwort, dass das Ganze zwar auf dem Papier geplant, in Tat und Wahrheit aber "dynamisch gewachsen" sei, dürfte wohl stellvertretend für viele andere genannt werden.

5.1.4 Zahlungsarten herkömmlich

Bei der Verwendung von herkömmlichen Zahlungsarten sind kaum Trends festzustellen. Die meisten Firmen bieten das ganze Sortiment von Vorauszahlung, über Kreditkarte bis Rechnung an, wobei offensichtlich das Bedürfnis nach einer gewissen Sicherheit bei den Firmen (Vorauszahlung!) verstärkt zum Vorschein kommt. Das Lastschriftverfahren wird von niemandem angeboten.

Die Vor- und Nachteile der herkömmlichen Verfahren werden ziemlich einheitlich beurteilt: Für den Einsatz spricht in erster Linie die grosse Verbreitung und damit kleine Schwellenangst der genannten Zahlungsarten. Bei den Nachteilen werden an erster Stelle die Debitorenverluste genannt, welche beim Verkauf auf Rechnung gerade bei kleinen Beträgen, wo sich eine Betreuung nicht lohnt, erheblich sind. Um diese Verluste zu verringern, wird entweder mehr Aufwand in die Bonitätsprüfung investiert oder aber auf andere Zahlungsarten wie Vorkasse oder Nachnahme zurückgegriffen. Diese Methoden sind allerdings bei den Kunden nicht beliebt.

Auf der Kostenseite werden grosse Handlinggebühren sowie der Inkassoaufwand als Negativpunkte genannt.

5.1.5 Zahlungsarten via Internet

Die mit Abstand am weitesten verbreitete Zahlungsart auf dem Internet ist die Belastung via Kreditkarte. Kreditkarten sind heute speziell bei Anwendern des Internets weit verbreitet und werden gut akzeptiert. Die Transaktionskosten werden nur selten als Nachteil genannt. Gesichert wird die Übertragung der Daten grösstenteils mittels SSL. Das Verfahren wird als sicher, weit verbreitet und kostengünstig beurteilt.

Durch den ecash Versuchsbetrieb der Swiss NetPay AG, siehe Kapitel 5.2.3, hat elektronisches Geld auch in der Schweiz Einzug gehalten. Da der Versuch

erst seit Anfang Juni 1998 läuft, hält sich die Erfahrung in engen Grenzen. Es wird ein Gesamtumsatz von deutlich unter einer Million Franken monatlich erwartet. Die wenigen Stimmen äusserten sich aber durchwegs positiv, an einen Ausstieg denkt zur Zeit niemand.

Das von den Kreditkartenfirmen stark propagierte SET ist zurzeit erst in einem Versuchsstadium. Dies liegt daran, dass in der Schweiz heute niemand eine Lösung basierend auf SET anbieten kann. Es ist allerdings damit zu rechnen, dass sich dies in nächster Zeit ändern wird.¹ Gerüchten zufolge, plant Migros den Einsatz von SET, was natürlich eine starke Signalwirkung hätte. Sparpotential besteht beim Übertrag der Daten in die Buchhaltung. Dies geschieht heute zum grössten Teil manuell. Integrierte Standardlösungen sind derzeit noch keine vorhanden und die Entwicklung einer eigenen Lösung ist für die kleineren Firmen zu teuer.

Von den befragten Firmen, welche noch keine Zahlungsmöglichkeiten via Internet anbieten, plant etwa die Hälfte mittelfristig den Einsatz von Kreditkartenlösungen oder ecash. Sie erhoffen sich davon eine Erleichterung des Inkassos, kleinere Debitorenverluste bei gesteigertem Umsatz und eine höhere Kundenzufriedenheit. Interessant ist auch eine Stimme, welche sich vom Einsatz dieser Zahlungsmittel die Erschliessung des internationalen Marktes erhofft. Die ablehnenden Stimmen begründeten ihre Haltung recht unterschiedlich: Bei grösseren Firmen war zu hören, dass der Umsatz via Internet zu unbedeutend sei, als dass sich Investitionen lohnen würden. Auch wurde eine Verunsicherung der Kunden, insbesondere was die Sicherheit betrifft, erwähnt. In einem Fall wurden die Kommissionen als zu hoch eingestuft.

5.1.6 Kosten und Nutzen

Zum Zeitpunkt der Befragung waren sämtliche Systeme zu wenig lange im Einsatz, um aussagekräftige Zahlen zu liefern. Grundsätzlich kann aber festgehalten werden, dass bisher keine grösseren Überraschungen eingetreten sind, offenbar waren die Anbieter genügend informiert.

5.1.7 Zahlungsumfang und Beträge

Ein Ziel der Umfrage war es, sowohl Umfang wie auch Struktur der Zahlungen via Internet zu erfassen.

Umsatzanteil

Der Umsatzanteil über das Internet ist je nach Firma stark unterschiedlich. Firmen, welche von Anfang an das Internet im Konzept berücksichtigten, erreichen über 50% des Umsatzes über dieses Medium. Bei den meisten anderen hingegen wird nur ein marginaler Anteil via Internet erzielt (maximal 10%). Die Tendenz ist steigend, E-Commerce gewinnt derzeit stark an Bedeutung.

Beträge

Die Grösse der Beträge bestimmt zu einem wichtigen Teil, welche Zahlungsarten Sinn machen. So verursachen z. B. Verkäufe auf Rechnung bei Beträgen unter Fr. 30.- viel zu hohe Kosten und zu grosse Debitorenverluste, während Systeme wie ecash für kleinere Beträge optimal sind.

Bei den in der Umfrage berücksichtigten Firmen dominieren die Beträge über

¹IBM macht zurzeit enorm Werbung für eine SET basierte Lösung

Fr. 50.-, kleine Beträge unter Fr. 10.- sind praktisch nicht vertreten. Bei den grösseren Beträgen ist einzig festzustellen, dass selten Zahlungen grösser als Fr. 500.- getätigt werden.

5.2 Anbieter von Zahlungssystemen

5.2.1 Reimer Internet Payment Systems AG

Die Reimer AG² bietet ein Payment System für E-Commerce an, welches Zahlungen per Kreditkarte, Rechnung und ecash ermöglicht. Ein Händler kauft dabei von der Reimer AG eine Dienstleistung, welche die komplette Zahlungstransaktion abdeckt.

Ablauf

Hat sich der Kunde für einen Kauf entschieden, übernimmt das Zahlungssystem von Reimer den Zahlungsablauf. Der Kunde entscheidet sich dialoggestützt für eine Zahlungsart und gibt die nötigen Angaben, wie z. B. die Kreditkartennummer, ein, welche vom System sofort geprüft werden. Dem Kunden wird per e-mail automatisch eine Quittung zugesandt.

In regelmässigen Abständen (typischerweise eine Woche) wird ein Clearing durchgeführt: Die kompletten Kreditkartentransaktionen werden ausgeführt und das Geld anschliessend als Gesamtbetrag dem Verkäufer überwiesen.

Transaktionen können vom Händler bis zum Clearing modifiziert oder abgebrochen werden. Ist ein Abbruch nach dem Clearing notwendig, muss eine individuelle Lösung zwischen Händler und Kunde gesucht werden. Bei ecash Transaktionen ist ein nachträglicher Abbruch nicht möglich.

Systeme und Währungen

Das System der Reimer AG verwendet grundsätzlich SSL zur Sicherung der Datenübertragung. Die Authentifikation gegenüber dem Kunden geschieht mittels Zertifikat, welches auf Reimer lautet - es ist nicht notwendig, dass jeder Kunde ein eigenes Zertifikat beantragt.

Die Implementation von ecash basiert auf den Libraries von DigiCash. Angeboten werden zur Zeit Schweizer Franken (ausgegeben von der Swiss NetPay AG) und US Dollar (ausgegeben von der Mark Twain Bank). Der Euro wird berücksichtigt, sobald er verfügbar wird. Weiter werden die üblichen Kreditkarten berücksichtigt.

Kosten

Bei der Verwendung des vorgestellten Systems entstehen, abhängig von den gewählten Optionen, Investitionskosten von ca. Fr. 4000.- bis Fr. 5000.-.

Zusätzlich zu den Gebühren des Systemanbieters (Kreditkarten 4%, ecash ca. 1.5 bis 2%), wird dem Händler pro Transaktion eine Kommission von ca. 2% verrechnet.

Bei der Verwendung von Kreditkarten muss der Verkäufer selber einen gültigen Vertrag mit der Kreditkartenfirma besitzen. Dies kann bei kleinem Umsatz zu zusätzlichen Fixkosten führen.³

Ein automatischer Übertrag in das Buchhaltungssystem ist mangels Standards nicht erhältlich. Ein entsprechendes System kann kundenspezifisch programmiert werden, was für kleinere Firmen kaum wirtschaftlich ist.

²<http://www.reimer.ch>

³siehe z. B. VISA Händlervertrag

5.2.2 The Blue Window (Swisscom)

The Blue Window⁴, kurz Bluewin, ist der Name für die Internet Dienste der Swisscom. Bluewin bietet sowohl Connectivity Dienste für Privatkunden und Firmen wie auch Web-Hosting und Consulting.

Ein spezieller Dienst stellt dabei die integrierte Gesamtlösung CommerceMaker⁵ dar. CommerceMaker ist eine Transaktionsplattform, welche sicheres Einkaufen und Bezahlen via Internet ermöglicht. Insbesondere besteht die Möglichkeit, Mikrotransaktionen via Kreditkarte oder Swisscom-Telefonrechnung zu belasten.

Kundenregistrierung

Um von den erweiterten Möglichkeiten von CommerceMaker Gebrauch zu machen, muss sich der Kunde registrieren. Ihm stehen dann die Möglichkeiten offen, Mikrotransaktionen zu tätigen, sowie seine Transaktionen des laufenden Monats zu überprüfen.

Ablauf

Ähnlich wie bei der Lösung der Reimer AG übernimmt CommerceMaker den kompletten ZV. Einzig beim Kauf auf Rechnung ist der Verkäufer für das Inkasso verantwortlich.

Zahlungsarten

CommerceMaker bietet folgende Zahlungsmöglichkeiten:

- Kreditkarte: VISA, MasterCard, American Express, Diners
- Swisscom Telefonrechnung
- Postkonto
- Rechnung
- Wallet⁶

Gesichert wird die Übertragung der Daten via SSL (mit 128 Bit Schlüssel).

Kosten

Die Installation von CommerceMaker kostet je nach Optionen in der Grössenordnung von Fr. 4500.- bis Fr. 15'000.-. Darin enthalten ist die Lizenz für die Software, das Einrichten sowie ein Tag Support. Weiter fallen monatliche Kosten zwischen Fr. 250.- und Fr. 350.- an.

Die Transaktionen sind je nach verwendeter Zahlungsart unterschiedlich. Bei Kreditkarten wird eine Kommission von 2% zusätzlich zu den Gebühren der Kreditkartenfirma verrechnet. Dasselbe gilt für Rechnungen. Mikrotransaktionen via Wallet werden mit 6% Kommission belastet.

⁴<http://www.bluewin.ch>

⁵<http://www.commercemaker.ch>

⁶Das "Wallet" ist ein elektronisches Portemonnaie, von welchem Mikrotransaktionen abgebucht werden.

5.2.3 Swiss NetPay AG

Der erste Versuch mit ecash in der Schweiz lief während der Entstehung dieser Arbeit an. Im Gegensatz zu den bisherigen ecash-Betreibern im Ausland (Mark Twain Bank, Deutsche Bank) ist die Swiss NetPay AG⁷ keine Bank, obwohl sie eine Tochtergesellschaft der Credit Suisse ist. Es handelt sich um ein Joint Venture zwischen der Credit Suisse und der ECOFIN AG. In diesem Sinne ist die Firma eigenständig, und ein Anschluss anderer Banken oder der Post ist nach der Pilotphase durchaus möglich und für die Kunden und Händler auch wünschenswert. Ähnlich wie bei den Kreditkartenherausgebern sollen Kunden und Händler sich nicht auf eine Bank festlegen müssen, um Ihren ZV abwickeln zu können.

Ablauf

Nach Eröffnung eines Kontos bei der Swiss NetPay transferiert der Kunde von seinem Bankkonto (in der Pilotphase nur bei der Credit Suisse) oder mittels Einzahlungsschein Geld auf sein ecash-Konto. Damit kann er nun bei den am Versuch angeschlossenen Händlern (ein Verzeichnis aller angeschlossenen Händler findet sich auf der Web-Seite der Swiss NetPay AG) einkaufen und mit ecash bezahlen. Die Händler haben ebenfalls ein Konto bei der Swiss NetPay AG auf welches ihnen die einbezahlten Beträge gutgeschrieben werden.

Kosten und Währung

Kosten entstehen den Kunden nur in Zusammenhang mit den Kommunikationskosten im Internet, mindestens während der Pilotphase ist die Benutzung des ecash-Kontos kostenlos.

Vorerst besteht nur die Möglichkeit, Konten in Schweizer Franken zu eröffnen. Dies dürfte sich nach der Pilotphase aber ändern. Das Geld auf dem ecash-Konto wird nicht verzinst. Zudem wird "jegliche Haftung [...] für Schäden, die dem Kunden durch die Benutzung des Internets erwachsen, wegbedungen".

⁷<http://www.swisspaynet.ch>

Kapitel 6

Zukunft des Internet-Zahlungsverkehrs

Prognosen für die Zukunft sind nur sehr bedingt abzugeben. Zuviele Unsicherheitsfaktoren sind in diesem schnelllebigen Geschäft vorhanden und die Abhängigkeiten vom gesamten E-Commerce lassen keine isolierten Betrachtungen zu. Sicher erscheint heute, dass sich der ZV via Internet auf lange Frist (auch) in der Schweiz durchsetzen wird.

Viele der Internet-ZV Pioniere wie beispielsweise First Virtual werden dabei wahrscheinlich auf der Strecke bleiben und durch konkurrenzfähigere und modernere Produkte ersetzt werden. Gute Erfolgsaussichten haben momentan sicherlich DigiCash mit ihrem Produkt ecash sowie Digital mit Millicent auf der Seite des elektronischen Geldes, und SET als Kreditkartenprodukt auf der anderen Seite des ZV-Spektrums im Bereich Kreditkarten-ZV.

Prognosen darüber, in welchem Zeitraum der ZV via Internet herkömmliche ZV-Produkte ernsthaft konkurrenzieren kann und wird, sind nur äusserst schwer zu machen. Einerseits muss das Internet seine Stellung als Kommunikationsmedium weiter ausbauen und Einzug in den Alltag einer breiten Bevölkerungsschicht finden, andererseits müssen die Kunden zu den angebotenen Produkten Vertrauen haben. Gerade dieses Kundenvertrauen in die neuen ZV-Technologien und E-Commerce kann mit wenigen Meldungen über Hacker und deren Einbrüche in Computersysteme sowie Missbräuche schwer geschädigt werden und die geleistete Arbeit wieder zunichtemachen.

Dem E-Commerce wird heute ein enormes Wachstumspotential zugeschrieben. Dieses kann aber nur realisiert werden, wenn auch die passenden Zahlungsmittel zur Verfügung stehen um auch international einfach einkaufen zu können. Durch die starke gegenseitige Abhängigkeit entsteht ein grosser Druck, die Systeme weiter zu entwickeln und zu fördern. Es ist zu erwarten, dass in Zukunft der ZV via Internet das Wachstum des gesamten E-Commerce erst richtig ermöglichen wird.

Die Systeme

Erst wenn sich die derzeitige Vielfalt von Systemen reduziert hat, wird ein breiter Einsatz der überlebenden Systeme möglich. Es gibt durchaus Platz für mehr als ein einziges System. Allerdings besteht kaum Platz für ein Nebeneinander von sich direkt konkurrenzierenden Systemen. Einen Schritt in die richtige Richtung haben dabei die Kreditkartenherausgeber mit ihrem SET Stand-

ard gemacht. Mehr Verwirrung herrscht im Moment bei der Verwendung von digitalem Geld (mit Systemen wie ecash oder Millicent) wo jede Bank ihr eigenes Geld ausgibt. Hier erinnert die Situation an die Schweiz vor 200 Jahren, als jeder Kanton seine eigene Wahrung hatte. Wie die Einfuhrung des Schweizer Frankens damals, und des Euro im EU-Raum heute, wird man auch auf dem Internet nicht daran vorbeikommen, allgemeingultiges Geld einzufuhren, d. h. von allen akzeptiertes Geld. Welche Produkte schlussendlich das Rennen machen werden, ist im Moment noch nicht abzusehen, auch wenn SET und ecash die Nase vorne haben. Millicent konnte sich als Zahlungssystem fur Mikropayments durchsetzen.

Die Unternehmen

Heute stellt die Abwicklung des ZV via Internet fur Unternehmen noch eine Moglichkeit zur Differenzierung und einen Wettbewerbsvorteil dar. Dies wird sich aber andern, Kunden werden in Zukunft negativ reagieren, wenn die Moglichkeit zur Bezahlung ubers Internet nicht gegeben ist. Insbesondere fur die Banken durfte ein Ausbau des Online-Bankings zur Pflicht werden. Ebenso muss die Post aufpassen, den Anschluss im ZV nicht zu verlieren. Die Kreditkartenunternehmen sind auf dem Gebiet des ZV via Internet am weitesten. Sie realisieren mit SET einen Standard, der alle jene Produkte verdrangen durfte, die sich ebenfalls mit der Abwicklung von Kreditkartentransaktionen befassen.

Eine Internetpresenz einschliesslich Presentation der Produkte, Bestellmoglichkeit und ZV lasst sich fur ein Unternehmen nicht von heute auf morgen realisieren. Je enger der firmeninterne Umgang mit digitalen Medien ist (Intranet), desto einfacher wird auch das "going public" ins Internet. Auch Mitarbeiter mussen auf die elektronischen Medien vorbereitet werden und sich damit identifizieren konnen. Neugegrundete Firmen, welche direkt in den Handel via Internet einsteigen, haben es hier gegenuber schon bestehenden sicher einfacher. Trotzdem bietet beispielsweise keines der schweizerischen, elektronischen Shoppingcenter die Bezahlung mittels ecash an oder nimmt am SET Versuch teil. Der Versuch der Swiss NetPay AG, mit immerhin 30 angeschlossenen Handlern, lasst fur die nahere Zukunft hoffen.

Zukunft in der Schweiz

Seit Anfangs 1998 ist in der Schweiz E-Commerce mehr als nur eine Randerscheinung, die Verkaufe via Internet steigen deutlich an. Damit steigt auch das Interesse am ZV ubers Internet. Es ware sicher zu optimistisch zu glauben, dass ecash wie in Australien oder Finnland bis zu 40% des Umsatzes via Internet ausmachen wird. Viele der befragten Firmen planen aber heute schon den Einsatz von ecash. Auch elektronisch gesicherte Kreditkartentransaktionen werden massiv gefordert.

Anhang A

Kryptographische Grundlagen

Dieser Anhang beschreibt die wichtigsten kryptographischen Konzepte und Protokolle, welche dem elektronischen ZV zugrunde liegen. Die Protokolle werden mit einigen Beispielen illustriert. Für eine detaillierte Erklärung der Protokolle sowie deren mathematische Grundlagen wird auf die Bücher von Schneider und van Orschrott (siehe Literaturverzeichnis) verwiesen.

“Applied Cryptography”, das Standardwerk der Kryptographie, vermittelt leicht verständlich einen allgemeinen Überblick über die Kryptographie und beleuchtet alle wichtigen Algorithmen.

Das “Handbook of Applied Cryptography” bietet einen breiten, mathematisch präzisen Einblick in die Kryptographie.

A.1 Definitionen

Die Wissenschaft der Kryptographie beinhaltet eine grosse Anzahl von Konzepten und Primitiven. Im folgenden werden diejenigen Begriffe und Konzepte eingeführt, welche für den elektronischen ZV von Bedeutung sind.

Kanal Ein Kanal ist eine beliebige Kommunikationsverbindung zwischen zwei Punkten. Dies kann eine Telefonlinie, eine Verbindung über das Internet oder auch ein Gespräch zwischen zwei Personen im selben Raum sein. In den folgenden Definitionen wird ein Kanal als unidirektional angenommen, bidirektionale Kanäle können leicht als zwei unidirektionale Kanäle modelliert werden. Weiter wird davon ausgegangen, dass die Verbindung immer von A (Alice) nach B (Bob) gerichtet ist. Kanäle können verschiedene Eigenschaften bezüglich der Sicherheit aufweisen, welche in den folgenden Abschnitten genau spezifiziert werden.

Die Zuverlässigkeit und Verfügbarkeit von Kanälen ist nicht Bestandteil dieser Einführung. Es wird davon ausgegangen, dass beliebig viele und zuverlässige Kanäle verfügbar sind.

Authentizität Ein Kanal ist authentisch, wenn Bob sicher sein kann, dass die empfangene Information von Alice und von keiner dritten Instanz stammt. Niemand ausser Alice kann erfolgreich auf dem Kanal senden. Die Authentifikation kann auf verschiedenen Methoden basieren, am Telefon z. B. indem

Bob die Stimme von Alice erkennt oder im Briefverkehr durch die Unterschrift oder ein Siegel von Alice.

Geheimhaltung Ein Kanal ist geheim, wenn nur Bob die von Alice gesendete Information empfangen kann. Ein Beispiel ist ein Briefkasten, zu welchem nur Bob den Schlüssel besitzt.

Sichere Kanäle Ein Kanal gilt als sicher, wenn sowohl die Geheimhaltung wie auch die Authentizität gewährleistet ist. Beispiel ist ein vertrauenswürdiger Kurier.

Hash-Funktion Ein Hash-Code ist das Resultat einer Einwegfunktion, welche einen grossen Attributraum auf einen kleinen Resultatraum abbildet (typischerweise eine 64 oder 128 Bit Zahl). Damit eine Hash-Funktion für kryptographische Zwecke verwendet werden kann, muss es unmöglich sein, für einen gegebenen Wert einen passenden Text zu konstruieren.

Kryptographisch sichere Hash-Funktionen lassen sich mit Hilfe eines symmetrischen Verschlüsselungsverfahrens leicht realisieren, indem nicht das gesamte Resultat, sondern nur die Bit-Summe modulo 2 (bitweises exklusives Oder) gespeichert wird. Ein effizienteres Verfahren ist beispielsweise MD5.

Attacken Wenn über Sicherheit von Kryptosystemen gesprochen wird, muss definiert werden, gegen welche Art von Gegner das System sicher sein soll. Dabei wird unterschieden zwischen passiven und aktiven Gegnern. Passive Gegner sind reine Zuhörer, welche, ohne den Protokollfluss zu ändern, versuchen, an Information zu kommen. Aktive Gegner hingegen können in das Protokoll eingreifen und z. B. falsche Daten einfügen.

Passive Gegner sind mit den verfügbaren Verfahren leicht auszuschalten, indem sämtliche Kommunikation verschlüsselt wird. Es besteht allerdings die Gefahr, dass ein Gegner die Kommunikation aufzeichnet und später wieder verwendet, um sich zum Beispiel bei einem System zu authentifizieren (Replay-Attack). Es genügt deshalb nicht, ein Passwort verschlüsselt zu übertragen.

Ein aktiver Gegner hat zusätzliche Möglichkeiten zur Verfügung: Er kann sich als Mittelsmann zwischen die Parteien schalten. Damit kann er sich gegenüber Alice als Bob ausgeben und gegenüber Bob als Alice. Gelingt ihm dies, kann er die gesamte Kommunikation zwischen den beiden Parteien abhören und verändern (man-in-the-middle-attack). Es ist deshalb wichtig, dass sich bei sämtlichen Transaktionen beide Parteien gegenseitig sicher authentifizieren.

Um ein Verschlüsselungsverfahren zu brechen, gibt es grundsätzlich folgende Methoden:

- **Brute-Force-Suche** Sämtliche möglichen Schlüssel werden getestet. Damit ein Treffer detektiert werden kann, muss der Ursprungstext oder zumindest dessen Struktur bekannt sein (Known-Plaintext). Dies ist allerdings sehr häufig der Fall: Datenformate und e-mails haben meist standardisierte Header.
- **Lineare Kryptoanalyse** In der linearen Kryptoanalyse werden Teile des Verschlüsselungsalgorithmus durch lineare Funktionen angenähert. Bei gewissen Algorithmen ist damit eine deutliche Verminderung der Komplexität möglich. Der enorm hohe Speicherbedarf bewirkt allerdings, dass eine solche Schwäche für die meisten Algorithmen von rein akademischem Interesse ist.

- **Differentielle Kryptoanalyse** Ähnlich wie in der linearen Kryptoanalyse werden in der differentiellen Kryptoanalyse Teile des Algorithmus durch einfachere Funktionen ersetzt - in diesem Falle werden allerdings Differenz-Funktionen eingesetzt. Auch diese Art der Analyse ist mehr akademischer Natur als von praktischer Relevanz.
- **Mathematische Verfahren:** Einige Verschlüsselungsverfahren basieren auf der Schwierigkeit, gewisse mathematische Probleme zu lösen. Für die entsprechenden Probleme existieren Algorithmen, welche unterschiedlich effizient sind (z. B. Primzahlzerlegung mit Hilfe von "Zahlen-sieben").

A.2 Symmetrische Verschlüsselung

Verschlüsselung verwandelt einen Klartext mit Hilfe eines Schlüssels in ein Chifftrat, welches über einen unsicheren Kanal übertragen werden kann. Ein Gegner kann den unsicheren Kanal abhören, hat aber ohne den Schlüssel keine Möglichkeit, aus dem empfangenen Chifftrat den ursprünglichen Klartext abzuleiten.

Symmetrisch ist eine Verschlüsselung dann, wenn sowohl die Chiffrierung wie auch die Dechiffrierung mit Hilfe desselben Schlüssels möglich ist. Der Schlüssel muss vorgängig über einen sicheren Kanal übertragen werden.

Ein mechanisches Analogon der symmetrischen Verschlüsselung ist ein Tresor, zu welchem sowohl Alice wie Bob den Schlüssel besitzen. Alice kann eine Nachricht im Tresor einschliessen mit dem Wissen, dass nur Bob diese holen kann. Bob kann weiter davon ausgehen, dass nur Alice die Nachricht in den Tresor gelegt haben kann, da nur sie den passenden Schlüssel besitzt. Symmetrische Verschlüsselung garantiert sowohl die Authentizität wie auch die Geheimhaltung einer Meldung.

A.2.1 Verfahren zur symmetrischen Verschlüsselung

Symmetrische Verschlüsselung wird seit vielen Jahren angewendet. Bekannte Beispiele gehen bis zu Julius Cäsar zurück, welcher für geheime Meldungen die Buchstaben permutierte. Die Enigma, welche von den Deutschen während des zweiten Weltkrieges verwendet wurde, ist ein weiteres bekanntes Beispiel. Heute existiert eine grosse Menge von Verfahren.

- **Data Encryption Standard, kurz DES**, wurde in den siebziger Jahren von IBM entwickelt und von der NSA¹ verbessert. DES permutiert einen 64 Bit Datenblock anhand eines 56 Bit Schlüssels. Es eignet sich in erster Linie zur Implementation in Hardware-Module. Der Schlüssel ist mit 56 Bit für heutige Sicherheitsanforderungen zu kurz. Mit einem speziell zu diesem Zweck gebauten Computer wäre es möglich, innerhalb weniger Minuten sämtliche möglichen Kombinationen zu prüfen. Bis heute ist nicht bekannt, ob ein solcher Computer tatsächlich gebaut wurde. Ein Chip-Entwurf, welcher den Bau für einige Millionen US Dollar ermöglicht, wurde Anfangs der neunziger Jahre veröffentlicht.
- **Triple-DES** Um die Key-Länge von DES auf 112 Bit zu verlängern, wurde das Triple-DES Verfahren entwickelt. Hierbei wird zuerst mit Schlüssel 1 verschlüsselt, danach mit Schlüssel 2 entschlüsselt und schliesslich

¹National Security Agency

wieder mit Schlüssel 1 verschlüsselt. Das Verfahren hat den Vorteil, kompatibel zu DES zu sein, wenn beide Schlüssel gleich gewählt werden. Triple-DES gilt heute als sicher.

- **IDEA** wurde zwischen 1990 und 1992 an der ETH durch X. Lai und J. Massey entwickelt. IDEA permutiert einen 64 Bit Datenblock anhand eines 128 Bit langen Schlüssels. Durch seinen Aufbau eignet sich IDEA speziell zur Software-Implementation. IDEA gilt heute als sicher: Die Schlüssellänge verunmöglicht eine brute-force Suche, systembedingte Schwächen wurden bisher keine gefunden.

A.3 Public-Key Kryptographie

Die Public-Key Kryptographie verwendet verschiedene Schlüssel zur Chiffrierung und Dechiffrierung. Der Schlüssel zur Chiffrierung wird öffentlich bekanntgegeben, derjenige zur Dechiffrierung hingegen kennt nur eine Person. Wenn Alice Bobs Public-Key kennt, kann sie eine Message damit verschlüsseln, welche nur Bob entschlüsseln kann. Es ist somit einfach möglich, einen geheimen Kanal herzustellen, ohne vorher einen sicheren Kanal zu benötigen. Über diesen geheimen Kanal kann Alice nun einen Schlüssel für ein symmetrisches Verfahren übermitteln und damit den Kanal zu einem sicheren Kanal machen. Wichtig ist aber zu beachten, dass sich Alice gegenüber Bob damit nicht authentifiziert hat. Ebenfalls beachtet werden muss, dass Bobs Public-Key authentisch sein muss.

Ein mechanisches Analogon zur Public-Key Kryptographie ist ein Vorhängeschloss, welches jedermann schliessen, aber nur derjenige öffnen kann, welcher den Schlüssel besitzt.

- **RSA** ist das heute gebräuchlichste Verfahren der Public-Key Kryptographie. Die Sicherheit von RSA basiert auf der Schwierigkeit, Primzahlzerlegung bei grossen Zahlen durchzuführen.
- **Elliptic Curves** sind ein weiteres Konzept, welches für die Public-Key Kryptographie verwendet wird. Der Vorteil dieses Verfahrens gegenüber RSA ist die effizientere Berechnung sowie die Tatsache, dass das Verfahren nicht patentiert ist.

A.4 Elektronische Unterschriften

Elektronische Unterschriften dienen zur Authentifizierung einer Meldung. Sie müssen folgende Bedingungen erfüllen:

- **Fälschungssicher** Wie eine herkömmliche Unterschrift sollten auch elektronische Unterschriften fälschungssicher sein. Im Gegensatz zu einer echten Unterschrift stellt sich allerdings das Problem der leichten Übertragbarkeit: Elektronisch gespeicherte Daten können einfach und ohne Hinterlassen irgendwelcher Spuren kopiert werden. Eine elektronische Unterschrift muss sich deshalb immer auf ein bestimmtes Dokument beziehen.
- **Einmaligkeit** Dieselbe Unterschrift darf nur für ein einziges Dokument gültig sein. Diese Forderung ist theoretisch nur erfüllbar, wenn das gesamte Dokument verschlüsselt in der Unterschrift enthalten ist. Dies ist in der Praxis wenig sinnvoll. Man beschränkt sich darauf, einen kryptographisch sicheren Hash-Code des Dokumentes zu verschlüsseln.

- **Überprüfbarkeit** Eine elektronische Unterschrift muss einfach und effizient überprüfbar sein. Bei Public-Key Systemen bedeutet dies, dass mit Hilfe eines authentischen Public-Keys die Unterschrift verifiziert werden kann.

A.4.1 RSA

Elektronische Unterschriften können einfach mittels RSA oder anderen, ähnlichen Public-Key Kryptosystemen erzeugt werden. Ein Hash-Code (z. B. MD5) wird mit dem Secret-Key verschlüsselt. Mit Hilfe des Public-Keys kann dieser Hash-Code entschlüsselt und damit verifiziert werden.

Blinde Unterschriften

Ein Spezialfall der elektronischen Unterschriften sind die blinden, elektronischen Unterschriften. Blind bedeutet, dass die unterschreibende Instanz nicht sieht, was sie unterschreibt. Mechanisches Analogon ist ein verschlossenes Couvert, welches ein Kohlenpapier im Inneren hat. Eine Unterschrift auf die Hülle wird damit auf das Dokument im Inneren transferiert, ohne dass der Unterschreibende das Dokument sehen kann.

Damit jemand ein Dokument blind unterschreibt, muss natürlich vorgängig bewiesen werden, dass das Dokument gültig ist. Dies kann z. B. damit realisiert werden, dass dem Unterschreiber k Dokumente übermittelt werden. Dieser verlangt die Öffnung von $k-1$ Dokumenten und verifiziert diese, das verbleibende, zufällig ausgewählte Dokument wird unterschrieben zurückgegeben. Die Betrugswahrscheinlichkeit ist damit $1/k$.

Zero-Knowledge Beweise

Interaktive Zero-Knowledge Beweise sind eine weitere, gebräuchliche Primitive der Kryptographie. Mit diesen Protokollen kann die Kenntnis von Information interaktiv bewiesen werden, ohne jedoch Angaben über die Information preiszugeben. Eine wichtige Eigenschaft ist die Interaktivität: Die Beweiskraft ist nur gegeben, während das Protokoll läuft. Es ist nicht möglich, die ausgetauschte Information aufzuzeichnen und später mit nur dieser Information den Beweis zu wiederholen.

Zero-Knowledge Beweise können zur Benutzerauthentisierung in On-Line Systemen verwendet werden. Mittels des Protokolls beweist der Benutzer die Kenntnis eines geheimen Schlüssels und damit seine Identität.

Fiat-Shamir Protokoll

Die Sicherheit des Fiat-Shamir Protokolls basiert auf dem Problem der Faktorisierung von $m = pq$, wobei p und q grosse Primzahlen sind. Alice wählt einen geheimen Wert S_a zufällig aus Z_m^* und veröffentlicht den Public-Key $P_a = (S_a)^2 \pmod{m}$.

Um die Kenntnis von S_a zu beweisen, sendet Alice zuerst ein "Commitment" $T = U^2$, wobei U zufällig aus Z_m^* ausgewählt wird. Anschliessend wählt Bob ein zufälliges Bit C und übermittelt dieses an Alice. Sie muss nun $R = U$ senden, falls $C = 0$, andernfalls muss sie $R = U * S_a$ senden. Bob prüft anschliessend, ob $R^2 = T * (P_a)^C$. Dieses Protokoll wird k mal wiederholt.

Bob ist nun aus folgendem Grund überzeugt, dass Alice S_a kennt: Jemand, der beide möglichen Challenges ($C = 0$ oder 1) beantworten kann, könnte aus den

Antworten S_a direkt und effizient berechnen. Ohne Kenntnis von S_a kann deshalb nur eine der Challenges korrekt beantwortet werden. Ein Betrüger wird damit mit Wahrscheinlichkeit 0.5 pro Runde entlarvt, nach k Runden ist die Wahrscheinlichkeit, nicht entlarvt zu werden 0.5^k .

Es ist wichtig, dass Bob die Challenge C zufällig wählt. Würde Alice C im Voraus, könnte sie sich entsprechend beim Senden von T darauf vorbereiten.

A.5 Sicherheit

Bei der Auswahl von Algorithmen der Kryptographie stellt sich stets die Frage nach der Sicherheit sowie deren Beweisbarkeit.

A.5.1 Informationstheoretische Sicherheit

Unter informationstheoretischer Sicherheit versteht man, dass selbst ein Gegner mit unendlichen Ressourcen nicht in der Lage ist, den korrekten Schlüssel zu finden respektive Aussagen über den Originaltext aus dem Chiffre abzuleiten.

Ein einfaches, informationstheoretisch sicheres Verfahren ist die sogenannte "One-Time-Pad-Verschlüsselung". Hierbei ist der geheime Schlüssel gleich lang wie die Meldung, das Chiffre ist die bitweise Summe modulo 2 (XOR) der Meldung und des Schlüssels. Der Schlüssel ist eine zufällige Bitfolge, welche z. B. durch Auswertung von quantenmechanischen Effekten (Transistorrauschen) gewonnen wird.

Sämtliche informationstheoretisch sicheren Verfahren sind mit enormen Aufwand verbunden, welcher den Einsatz nur bei Anwendungen von allerhöchster Bedeutung rechtfertigt (z. B. heisser Draht Washington - Moskau während des kalten Krieges).

A.5.2 Berechenmässige Sicherheit

Die meisten gebräuchlichen Algorithmen bieten nur berechenmässige Sicherheit. Dies bedeutet, dass ein Gegner mit beschränkten Ressourcen nicht in der Lage ist, innert nützlicher Frist den Schlüssel oder den Klartext zu finden. Es wäre allerdings theoretisch möglich, den Schlüssel zu finden. Die gebräuchlichen Verfahren basieren entweder darauf, dass der komplette Schlüsselraum getestet werden müsste (z. B. 128 Bit bei IDEA ergibt 2^{128} mögliche Kombinationen) oder aber auf der Schwierigkeit, ein bestimmtes mathematisches Problem zu lösen (Faktorisierung von grossen Zahlen bei RSA oder diskreter Logarithmus). Die Sicherheit dieser Algorithmen nimmt mit der Zunahme der verfügbaren Rechenleistung durch den technischen Fortschritt ab, so dass stets eine gewisse Sicherheitsmarge eingerechnet werden muss.

A.5.3 Beweisbarkeit

Die Sicherheit eines Algorithmus zu beweisen, ist häufig nicht möglich. Keiner der hier aufgeführten, symmetrischen Algorithmen ist als sicher bewiesen. DES wurde aber über viele Jahre hinweg von unabhängigen Kryptoanalysten praktisch erfolglos zu knacken versucht. Die differentielle Kryptoanalyse zeigte gewisse Möglichkeiten zum Brechen des Algorithmus auf, diese sind allerdings infolge enormen Speicherbedarfes eher akademischer Natur. Ähnliches gilt für IDEA, wobei hier auch die differentielle Kryptoanalyse versagt.

Anders sieht die Situation bei den Public-Key Algorithmen aus. Hier basieren

die meisten Algorithmen auf der Schwierigkeit der Primzahlfaktorisation. Im Falle von RSA wird angenommen, bei Elliptic-Curves-Systemen ist bewiesen, dass die Komplexität äquivalent ist. Es ist nicht auszuschließen, dass irgendwann eine effiziente Lösung gefunden wird.

Zusammenfassend kann festgehalten werden, dass die Sicherheit von allen verbreiteten, kryptographischen Systemen zwar nicht bewiesen ist, im allgemeinen aber für mindestens 10 Jahre als genügend eingestuft werden kann. Problematisch sind die US Exportrestriktionen, welche den Export von sämtlichen sicheren Systemen verbieten.

Anhang B

Fragebogen

B.1 Firmen mit elektronischen Zahlungsmöglichkeiten

Der folgende Fragebogen wurde an diverse Firmen per e-mail versandt, welche bereits auf dem Internet präsent sind und Zahlungen auf elektronischem Weg ermöglichen.

Sehr geehrte Damen und Herren

Im Rahmen unserer Semesterarbeit an der ETH Zuerich am Lehrstuhl fuer Betriebswirtschaft behandeln wir das Thema "Zahlungsverkehr via Internet in der Schweiz". Wir moechten eine Bestandesaufnahme der momentan eingesetzten Systeme durchfuehren und die Systeme miteinander vergleichen. Die gewonnenen Erkenntnisse sollen helfen, den Zahlungsverkehr via Internet populaerer zu machen. Wir waeren Ihnen sehr dankbar, wenn Sie uns dabei mit der Beantwortung der folgenden Fragen unterstuetzen wuerden. Wie wir Ihrem Internet-Auftritt entnehmen, bieten Sie Ihren Kunden die Moeglichkeit an, die bei Ihnen bestellten Waren via Internet auch gleich zu bezahlen. Wir moechten Sie daher bitten, den Fragebogen zu beantworten oder, falls die Fragen nicht in Ihren Verantwortungsbereich fallen, an die zustaeendigen Stellen in Ihrer Firma weiterzuleiten. Das Ausfuellen des Fragebogens beansprucht ca. 15-20 Minuten.

1 Allgemeine Fragen zum Zahlungsverkehr via Internet

1.1 Wie lange ist Ihre Firma schon mit dem Internet vertaut?

[] Jahre

1.2 Welche der folgenden Begriffe sind Ihnen bekannt

[] Internet

[] Java

[] Applet

[] Digitales Geld

[] SSL

1.3 Sehen Sie Chancen und/oder Gefahren fuer Ihre Firma im

Internet?

2 Einfuehrung eines Produkts fuer den Zahlungsverkehr via Internet

2.1 Wie eng war Ihre Firma vor dem Einsatz von Internet Zahlungsmoeglichkeiten mit elektronischen Medien verbunden, hatten Sie beispielsweise schon vorher ein Intranet oder kommunizierten Ihre Mitarbeiter ueber e-mail miteinander?

2.2 Wer sprach das Thema eines Internet-Auftritts Ihrer Firma an?

2.3 Wer entschied ueber die Einfuehrung?

2.4 Wer realisiert die Einfuehrung?

- Firmeneigene Informatik
- Marketingabteilung mit Fremdhilfe
- Marketingabteilung mit eigener Informatik
- andere:

2.5 Wurden Sie durch Partner beraten?

2.6 Welches waren Ihre wichtigsten Etappen auf dem Weg zu Ihrem Internet-Auftritt in der aktuellen Form?

3 Zahlungsarten

3.1 Welche herkoemmlichen Zahlungsarten bieten Sie Ihren Kunden bei Kaeufen uebers Internet an?

- LSV
- Einzahlungsschein
- Kreditkarte uebers Telefon
- Per Nachnahme
- andere:

3.2 Welches Produkt fuer den Zahlungsverkehr via Internet setzten sie ein?

- SSL
- SET
- ecash
- First Virtual
- andere:

3.3 Wie und warum wurde der Entscheid zugunsten dieses Produkts gefaellt?

3.4 Wie zuverlaessig arbeitet Ihr System fuer den Zahlungsverkehr? Hatten Sie groessere Pannen, etwa bei der Einfuehrung?

3.5 Welche anderen Systeme kennen Sie/wurden von Ihnen evaluiert?

- SSL

- SET
- ecash
- First Virtual
- andere:

3.5 Wie wickeln Sie die uebers Netz bezahlten Geschaefte in Ihrer Buchhaltung ab?

- Manuelle Uebertragung ins Buchhaltungssystem
- Elektronisch ueber Datentraeger
- Direkter Zugang ins Buchhaltungssystem
- andere:

4 Kosten/Nutzen

4.1 Welche Kosten sind bei der Einfuehrung des Systems entstanden? Welche laufenden Kosten haben Sie mit Ihrem System und wie sehen diese Kosten im Vergleich zu den Kosten fuer den herkoemmlichen Zahlungsverkehr aus?

4.2 Welchen Nutzen haben Sie sich am Anfang versprochen? Welcher Nutzen ist tatsaechlich entstanden?

4.3 Welche Kommunikationsmittel haben Sie verwendet/verwenden Sie, um auf Ihre Zahlungsmoeglichkeiten via Internet aufmerksam zu machen?

- Rundschreiben an Kunden per Post
- Rundschreiben an Kunden via e-mail
- Hinweise um Katalog
- Hinweise auf der Web-Seite
- andere:

4.4 Unterstuetzen Sie die Bezahlung via Internet mittels Verkaufsfoerderung?

- Coupon
- Rabatte
- Praemien
- andere:

4.5 Entspricht der erzielte Gewinn/Verlust Ihren Erwartungen?

- JA NEIN
- Verlust Gewinn

5 Kunden

5.1 Kann der Kunde eine Bestellung und insbesondere die Bezahlung rueckgaengig machen? Falls ja, wie wird dies bei Ihnen gehandhabt? Falls nein, warum nicht?

5.2 In welcher Groessenordnung sind die von Kunden bezahlten Einzelbeträge?

- <10 CHF
- 10 - 50 CHF
- 50 - 100 CHF
- 100 - 500 CHF

] > 500 CHF

5.3 Wieviele Ihrer Kunden benutzen die elektronische Zahlungsmoeglichkeit?

-] < 1 %
-] 1 - 5 %
-] 5 -10 %
-] 10 50 %
-] > 50 %

5.4 Hat sich dieses Verhaeltnis seit der Einfuehrung bis heute veraendert?

-] mehr Bezahlungen uebers Internet
-] gleichbleibend
-] weniger Bezahlungen uebers Internet

5.5 Wieviele Prozent Ihres Geschaefitsumsatzes machen Sie ungefaehr uebers Internet?

-] < 1 %
-] 1 - 5 %
-] 5 -10 %
-] 10 - 50 %
-] > 50 %

5.6 Wieviele Prozent davon werden direkt uebers Internet bezahlt?

-] < 5 %
-] 5 - 10 %
-] 10 -50 %
-] > 50 %

5.7 Wie sieht das Verhaeltnis zwischen herkoemmlichen Zahlungstransaktionen und Zahlungstransaktionen via Internet aus?

6 Zukunft

6.1 Wo sehen Sie die entscheidenden Vorteile eines Einsatzes von Produkten fuer den Zahlungsverkehr via Internet?

6.2 Werden Sie weitermachen?

7 Ihre Firma

7.1 Welche Produkte stellen Sie her/vertreiben Sie?

7.2 Welche davon verteiben Sie via Internet?

7.3 Welche Groesse hat Ihr Unternehmen?

-] Einzelhandels-gesellschaft
-] KMU
-] Grossbetrieb

7.4 Waeren Sie bereit, uns weitere Auskuenfte zu geben?

Telefonisch

Gespraech

7.5 Duerfen wir Sie in unserem Bericht namentlich und mit
Ihren Angaben erwaehnen, oder moechten sie anonym bleiben?

Namentlich Anonym

Wir moechten Ihnen jetzt schon dafuer danken, dass Sie
sich Zeit genommen haben, die Fragen zu beantworten.

Mit freundlichen Gruessen

Martin Naef und Oliver Separovic

B.2 Firmen ohne elektronische Zahlungsmöglichkeit

Der folgende Fragebogen wurde an Firmen per e-mail versandt, welche zwar auf dem Internet präsent sind, aber keine Zahlungsmöglichkeit auf elektronischem Weg ermöglichen.

Sehr geehrte Damen und Herren

Im Rahmen unserer Semesterarbeit an der ETH Zuerich am Lehrstuhl fuer Betriebswirtschaft behandeln wir das Thema "Zahlungsverkehr via Internet in der Schweiz". Wir moechten eine Bestandesaufnahme der momentan eingesetzten Systeme durchfuehren und die Systeme miteinander vergleichen. Die gewonnenen Erkenntnisse sollen helfen, den Zahlungsverkehr via Internet populaerer zu machen. Wir waeren Ihnen sehr dankbar, wenn Sie uns dabei mit der Beantwortung der folgenden Fragen unterstuetzen wuerden.

Wie wir Ihrem Internet-Auftritt entnehmen, bieten Sie Ihren Kunden die Moeglichkeit an, Waren ueber Internet zu bestellen. Sie verzichten bisher aber darauf, Ihren Kunden die Moeglichkeit zu geben, direkt uebers Internet zu bezahlen. Uns wuerde interessieren, warum. Wir moechten Sie daher bitten, den Fragebogen zu beantworten oder, falls die Fragen nicht in Ihren Verantwortungsbereich fallen, an die zustaendigen Stellen in Ihrer Firma weiterzuleiten. Das Ausfuellen des Fragebogens beansprucht ca. 10 Minuten.

- 1 Allgemeine Fragen zum Zahlungsverkehr via Internet
 - 1.1 Wie lange ist Ihre Firma schon mit dem Internet vertaut?
 Jahre
 - 1.2 Wie eng ist Ihre Firma mit elektronischen Medien verbunden, haben Sie beispielsweise ein Intranet oder kommunizieren Ihre Mitarbeiter ueber e-mail miteinander?
 - 1.3 Welche der folgenden Begriffe sind Ihnen bekannt?
 Internet
 Java
 Applet
 Digitales Geld
 SSL
 - 1.4 Sehen Sie Chancen und/oder Gefahren fuer Ihre Firma im Internet?
- 2 Planung und Einfuehrung Ihres Internet-Auftrittes
 - 2.1 Wer sprach das Thema eines Internet-Auftritts Ihrer Firma an?

2.2 Wer entschied ueber die Einfuehrung?

2.3 Wer realisiert die Einfuehrung?

- Firmeneigene Informatik
- Marketingabteilung mit Fremdhilfe
- Marketingabteilung mit eigener Informatik
- andere:

2.4 Wurden Sie durch Partner beraten?

2.5 Welches waren Ihre wichtigsten Etappen auf dem Weg zu Ihrem Internet-Auftritt in der aktuellen Form?

3 Zahlungsarten

3.1 Welche Zahlungsarten bieten Sie Ihren Kunden bei Kaeufen uebers Internet an?

- LSV
- Einzahlungsschein
- Kreditkarte uebers Telefon
- Per Nachnahme
- andere:

3.2 Worin sehen Sie die Vorteile der gewaehlten Zahlungsarten? Nachteile?

3.3 Welche Produkte fuer den Zahlungsverkehr via Internet kennen Sie?

- SSL
- SET
- ecash
- First Virtual
- andere:

3.4 Planen Sie den Einsatz einer oder mehrerer der oben genannten Zahlungsarten?

Falls nein, warum nicht?

3.5 Falls Sie den Einsatz von Internetzahlungsmitteln planen: Welchen Nutzen versprechen Sie sich?

5 Kunden

5.1 In welcher Groessenordnung sind die von Kunden bezahlten Einzelbeträge bei Bestellungen uebers Internet?

- <10 CHF
- 10 - 50 CHF
- 50 - 100 CHF
- 100 - 500 CHF
- > 500 CHF

5.2 Wieviele Prozent Ihres Geschaefhtsumsatzes machen Sie ungefaehr uebers Internet?

- < 1 %
- 1 - 5 %
- 5 -10 %
- 10 - 50 %
- > 50 %

6 Ihre Firma

6.1 Welche Produkte stellen Sie her/vertreiben Sie?

6.2 Welche davon verteiben Sie via Internet?

6.3 Welche Groesse hat Ihr Unternehmen?

- Einzelhandels-gesellschaft
- KMU
- Grossbetrieb

6.4 Waeren Sie bereit, uns weitere Auskuenfte zu geben?

- Telefonisch
- Gespraech

6.5 Duerfen wir Sie in unserem Bericht namentlich und mit Ihren Angaben erwaehnen, oder moechten sie anonym bleiben?

- Namentlich Anonym

Wir moechten Ihnen jetzt schon dafuer danken, dass Sie sich Zeit genommen haben, die Fragen zu beantworten.

Mit freundlichen Gruessen

Martin Naef und Oliver Separovic
mnaef@iic.ethz.ch / oseparator@iic.ethz.ch

B.3 Auswertung

B.3.1 Firmen mit Internetzahlungsmitteln

Der folgende Abschnitt listet die Antworten der Firmen auf, welche bereits heute Zahlungsverkehr via Internet anbieten. In den eckigen Klammern steht jeweils die Anzahl der Händler, welche das betreffende Feld angekreuzt haben. Total haben 5 Firmen geantwortet.

Auf einige Fragen wird nicht eingegangen, da keine verwertbaren Angaben erhältlich waren.

1 Allgemeine Fragen zum Zahlungsverkehr via Internet

1.1 Wie lange ist Ihre Firma schon mit dem Internet vertraut?

1, 3, 2 (0.5 Shop), 1, 1

1.2 Welche der folgenden Begriffe sind Ihnen bekannt?

[5] Internet
 [5] Java
 [4] Applet
 [5] Digitales Geld
 [4] SSL

1.3 Sehen Sie Chancen und/oder Gefahren fuer Ihre Firma im Internet?

keine Gefahren 3
 von Anfang an dabei! 1
 Praktisch nur e-commerce! 1

2 Einfuehrung eines Produkts fuer den Zahlungsverkehr via Internet

2.1 Wie eng war Ihre Firma vor dem Einsatz von Internet Zahlungsmoeglichkeiten mit elektronischen Medien verbunden, hatten Sie beispielsweise schon vorher ein Intranet oder kommunizierten Ihre Mitarbeiter ueber e-mail miteinander?

e-mail 1
 Intranet 2
 Nicht 2

2.2 Wer sprach das Thema eines Internet-Auftritts Ihrer Firma an?

internet Gespraechе 1
 chef 1
 Geschaeftsfuehrung & Marketing 1
 Geschaeftsfuehrer 2

2.3 Wer entschied ueber die Einfuehrung?

Geschaeftsfuehrer 1

Geschaeftsfuehrung & Marketing 1
 Geschaeftsleitung 2

2.4 Wer realisiert die Einfuehrung?

[2] Firmeneigene Informatik
 [1] Marketingabteilung mit Fremdhilfe
 [] Marketingabteilung mit eigener Informatik
 [1] andere: Externe Informatikfirma, externer
 Informatiker
 [1] Shopmaker
 [1] Hunziker EDV

2.5 Wurden Sie durch Partner beraten?

nein 1
 ja 4

3 Zahlungsarten

3.1 Welche herkoemmlichen Zahlungsarten bieten Sie Ihren Kunden bei Kaeufen uebers Internet an?

[] LSV
 [4] Einzahlungsschein
 [3] Kreditkarte uebers Telefon
 [3] Per Nachnahme
 [2] andere: Kreditkarten uebers Internet

3.2 Welches Produkt fuer den Zahlungsverkehr via Internet setzten Sie ein?

[3] SSL
 [] SET (in Planung 1x)
 [4] ecash
 [] First Virtual
 [] andere:

3.3 Wie und warum wurde der Entscheid zugunsten dieses Produkts gefaellt?

- Erfahrung,
 - schwierig zu entschluesseln (SSL)
 - SSL ist Standard
 - ecash von Kunden vorgeschlagen
 - ecash Aufnahme in Pilot 2
 - SET und e-cash wird Standard
 - Verbindung zur CS

3.5 Welche anderen Systeme kennen Sie/wurden von Ihnen evaluiert?

[3] SSL
 [2] SET

- ecash
- First Virtual
- andere:

3.5 Wie wickeln Sie die uebers Netz bezahlten Geschaefte in Ihrer Buchhaltung ab?

- Manuelle Uebertragung ins Buchhaltungssystem
- Elektronisch ueber Datentraeger
- Direkter Zugang ins Buchhaltungssystem
- andere:

4 Kosten/Nutzen

4.1 Welche Kosten sind bei der Einfuehrung des Systems entstanden? Welche laufenden Kosten haben Sie mit Ihrem System und wie sehen diese Kosten im Vergleich zu den Kosten fuer den herkoemmlichen Zahlungsverkehr aus?

- | | |
|--------------------|---|
| keinen Unterschied | 2 |
| noch keine Angaben | 2 |

4.2 Welchen Nutzen haben Sie sich am Anfang versprochen? Welcher Nutzen ist tatsaechlich entstanden?

- | | |
|---------------------------------|---|
| Erleichterung | 1 |
| Kundennutzen, intern bescheiden | 1 |
| Zu frueh... | 1 |

4.3 Welche Kommunikationsmittel haben Sie verwendet/verwenden Sie, um auf Ihre Zahlungsmoeglichkeiten via Internet aufmerksam zu machen?

- Rundschreiben an Kunden per Post
- Rundschreiben an Kunden via e-mail
- Hinweise um Katalog
- Hinweise auf der Web-Seite
- andere:

4.4 Unterstuetzen Sie die Bezahlung via Internet mittels Verkaufsfoerderung?

- Coupon
- Rabatte
- Praemien
- andere:

4.5 Entspricht der erzielte Gewinn/Verlust Ihren Erwartungen?

- JA NEIN
- Verlust Gewinn

5 Kunden

5.1 Kann der Kunde eine Bestellung und insbesondere die Be-

zahlung rueckgaengig machen? Falls ja, wie wird dies bei Ihnen gehandhabt? Falls nein, warum nicht?

- ja
- ja Annullierung Online
- ja innert 30 Tagen, Kunde erhaelt Gutschrift

5.2 In welcher Groessenordnung sind die von Kunden bezahlten Einzelbeträge?

- <10 CHF
- [1] 10 - 50 CHF
- [2] 50 - 100 CHF
- [2] 100 - 500 CHF
- > 500 CHF

5.3 Wieviele Ihrer Kunden benutzen die elektronische Zahlungsmoeglichkeit?

- [1] < 1 %
- [1] 1 - 5 %
- [1] 5 -10 %
- [] 10 50 %
- [1] > 50 %

5.4 Hat sich dieses Verhaeltnis seit der Einfuehrung bis heute veraendert?

- [3] mehr Bezahlungen uebers Internet
- [1] gleichbleibend
- [] weniger Bezahlungen uebers Internet

5.5 Wieviele Prozent Ihres Geschaefitsumsatzes machen Sie ungefaehr uebers Internet?

- [1] < 1 %
- [1] 1 - 5 %
- [1] 5 -10 %
- [] 10 - 50 %
- [1] > 50 %

5.6 Wieviele Prozent davon werden direkt uebers Internet bezahlt?

- [1] < 5 %
- [1] 5 - 10 %
- [1] 10 -50 %
- [1] > 50 %

5.7 Wie sieht das Verhaeltnis herkoemmllicher Zahlungstransaktionen und Zahlungstransaktionen via Internet aus?

wird noch eingefuehrt

groesster Teil EZ, Rest Internet
< 1%
1000 : 1

6 Zukunft

6.1 Wo sehen Sie die entscheidenden Vorteile eines Einsatzes von Produkten fuer den Zahlungsverkehr via Internet?

Versandhandel!
Einfaches Handling waere Vorteil, ist aber noch nicht der Fall
Sicherheit / Dienstleistung
Keine Gebuehren, Geld wird direkt abgebucht, kein Risiko

6.2 Werden Sie weitermachen?

ja, auf jeden Fall! 5

7 Ihre Firma

7.1 Welche Produkte stellen Sie her/vertreiben Sie?

Hard/Software, Spiele, Buecher, Fax, Telefon
Werbung, Fotostudio, Internet
CD, Video, DVD, Games, CD-ROM, Standardsoftware
Schokoladespezialitaeten
Einzigartige Produkte, Neuheiten per Versand und in Laeden

7.2 Welche davon verteiben Sie via Internet?

alle 4

7.3 Welche Groesse hat Ihr Unternehmen?

[] Einzelhandelsgesellschaft
[5] KMU
[] Grossbetrieb

B.3.2 Firmen ohne Internetzahlungsmittel

Der folgende Abschnitt listet die Antworten der Firmen auf, welche noch keinen Zahlungsverkehr via Internet anbieten. Total haben 14 Firmen geantwortet.

1 Allgemeine Fragen zum Zahlungsverkehr via Internet

1.1 Wie lange ist Ihre Firma schon mit dem Internet vertraut?

[3x1j, 1.5, 5x2j, 3, 3.5, 4, 1, 5] Jahre

1.2 Wie eng ist Ihre Firma mit elektronischen Medien verbunden, haben Sie beispielsweise ein Intranet oder kommunizieren Ihre Mitarbeiter ueber e-mail miteinander?

e-mail	6
Intranet	4
nein	2

1.3 Welche der folgenden Begriffe sind Ihnen bekannt?

[14] Internet
 [13] Java
 [9] Applet
 [9] Digitales Geld
 [8] SSL

1.4 Sehen Sie Chancen und/oder Gefahren fuer Ihre Firma im Internet?

+ kleine Firma, grosser Markt
 + Neue Kunden, Umsatzsteigerung
 + Reduktion administrativer Aufwand
 + Weniger Fehler bei Bestellaufnahme
 + Chancen!
 + Wenig Investition, grosse Wirkung
 + Kostenguenstiger Auftritt
 - Hacker
 - Gefahr: Ueber/Unterschaetzung der Bedeutung
 - Attacken via Homepage: Rufschaedigung, falsche e-mails etc.

2 Planung und Einfuehrung Ihres Internet-Auftrittes

2.1 Wer sprach das Thema eines Internet-Auftritts Ihrer Firma an?

Geschaeftsleitung	6
4 Partner	
EDV-Verantwortlicher	
Von Anfang an Teil des Firmenkonzeptes	
Marketing	
Internet-Partner	

2.2 Wer entschied ueber die Einfuehrung?

4 Partner	
Geschaeftsleiter und EDV Verantwortlicher	
Geschaeftsleitung	7
Verwaltungsrat	3

2.3 Wer realisiert die Einfuehrung?

<input type="checkbox"/> [6] Firmeneigene Informatik	
<input type="checkbox"/> [6] Marketingabteilung mit Fremdhilfe	
<input type="checkbox"/> [] Marketingabteilung mit eigener Informatik	
<input type="checkbox"/> [] andere:	www.delta.ch
	Kaufmaennischer Leiter
	selber
	Internet-Partner

2.4 Wurden Sie durch Partner beraten?

ja	10
nein	4

3 Zahlungsarten

3.1 Welche Zahlungsarten bieten Sie Ihren Kunden bei Kaeufen uebers Internet an?

<input type="checkbox"/> [] LSV	
<input type="checkbox"/> [9] Einzahlungsschein	
<input type="checkbox"/> [8] Kreditkarte uebers Telefon / Fax	
<input type="checkbox"/> [6] Per Nachnahme	
<input type="checkbox"/> [] andere:	VISA/Mastercard ueber Internet
	Geld gegen Ware
	Vorauskasse 2
	Rechnung, Absicherung Kreditkarte
	oder Fax
	Barzahlung in Couvert

3.2 Worin sehen Sie die Vorteile der gewaehlten Zahlungsarten? Nachteile?

- + Wahlmoeglichkeit des Kunden
- + Kundenfreundliche, unkompliziert, keine Schwellenangst
- + Beliebt, verbreitet
- + Keine zusaetzlichen Aufwendungen
- + Geld sofort, keine Mahnungen
- Sicherheit bei Kreditkartendaten
- Debitorenkontrolle bei Rechnungen
- Geld gegen Ware: Kein Risiko, Kunde muss aber zuhause sein
- Groesserer Aufwand, da Bonitaetspruefung noetig
- Debitorenverluste
- NN unbeliegt, direktzahlung generiert mehr Umsatz
- Sicherheit

- Hohe Gebuehren
- Kontrolle, Mahnwesen
- Scherzbestellungen (EZ)
- Aufwendig im Handling

3.3 Welche Produkte fuer den Zahlungsverkehr via Internet kennen Sie?

- [6] SSL
- [7] SET
- [8] ecash
- [1] First Virtual
- [] andere:

3.4 Planen Sie den Einsatz einer oder mehrerer der oben genannten Zahlungsarten? Falls nein, warum nicht?

- Spontanitaet des Kunden jederzeit noetig
- Kommission zu hoch
- Unsicherheitsfaktor
- Sicherheit
- zu teuer
- Verunsicherung des Volkes durch Medien
- zu kleiner Umsatz via Internet 2
- Information - sobald mehr verfuegbar, wird es Alternative

- Ja - saemtliche Verfuegbaren
- Ja - SET 2
- Ja - e-cash 1
- SSL laeuft bereits
- Ja 2
- nein 1

3.5 Falls Sie den Einsatz von Internetzahlungsmitteln planen: Welchen Nutzen versprechen Sie sich?

- Kundenzufriedenheit, Arbeitserleichterung,
- Nutzung vorhandener Technologien
- Keine Nachnahmen, COD...
- Mehr Umsatz
- Sicher, einfach
- Groessere Akzeptanz bei SET
- Einfacheres Inkasso
- Lieferungen ins Ausland moeglich
- Innovatives Erscheinungsbild gegenueber Kunden
- Geringerer Handlingaufwand

5 Kunden

5.1 In welcher Groessenordnung sind die von Kunden bezahlten Einzelbeträge bei Bestellungen uebers Internet?

- [] <10 CHF

- [1] 10 - 50 CHF
- [7] 50 - 100 CHF
- [9] 100 - 500 CHF
- [4] > 500 CHF

5.2 Wieviele Prozent Ihres Geschaefitsumsatzes machen Sie ungefaehr uebers Internet?

- [2] < 1 %
- [5] 1 - 5 %
- [2] 5 -10 %
- [2] 10 - 50 %
- [3] > 50 %

6 Ihre Firma

6.1 Welche Produkte stellen Sie her/vertreiben Sie?

Haushaltwaren / Geraete
Fahrradbestandteile, Sportartikel
Lebensmittelbereich
Elektrowerkzeuge
Computer - Komponenten
Computer - Peripherie
High-End Audio, CDs
Buecher, Multimedia / Software
Buecher, Medien
Hochwertige Nahrungsmittel
CDs
Dienstleistung Blumenvermittlung
Textilien
Visitenkarten, Stempel, Kleber, Drucksachen
Weine Fuer Geniesser
Astrologische Analysen
Gesamtloesungen fuer Kleinunternehme (MS-Access)

6.2 Welche davon verteiben Sie via Internet?

Teilsortiment
Teilsortiment Food
Ausgewaehlte Produkte und Zubehoer (Service)
Alle 10

6.3 Welche Groesse hat Ihr Unternehmen?

- [5] Einzelhandelsgesellschaft
- [8] KMU
- [1] Grossbetrieb

Literaturverzeichnis

- [1] N. Asokan, Doktorarbeit "Fairness in Electronic Commerce", Universität von Waterloo, 1998
- [2] Committee on Payment and Settlement Systems, "Statistics on Payment Systems in the Group of Ten Countries", Bank for International Settlements, 1996
- [3] P. Frazer, "Plastic and Electronic Money: New Paymentsystems and their Implications", Woodhead-Faulkner, Cambridge, 1985
- [4] A. Furche und G. Wrightson, "Computer Money", dpunkt, 1996
- [5] Ch. Hirszowicz, "Schweizerische Bankpolitik", Verlag Paul Haupt, Bern 1996
- [6] Ph. Janson und M. Waidner, "Electronic Payment over Open Networks", INFORMATIK, 3/1995
- [7] D. Kunz, Seminar Informatik und Recht "Rechtsfragen der Applikation Ecash", Universität Zürich, 1997
- [8] G. D. Lehmann, "Zahlungsverkehr der Banken", Verlag des Schweizerischen kaufmännischen Verbandes, Zürich, 1985
- [9] D. Lynch, "digital money", John Wiley & Sons, Inc., 1996
- [10] P. van Orschrott et al., "Handbook of Applied Cryptography", CRC Press, 1996
- [11] K. Schaufelberger, "Kartengestützte Zahlungssysteme", Peter Lang AG, 1995
- [12] B. Schneier, "Applied Cryptography, Second Edition", John Wiley & Sons, 1996
- [13] A. Seiler, "Marketing", Orell Füssli, Zürich 1992
- [14] K. Spremann, "Wettbewerb und Technologie im Zahlungsverkehr", Verlag Paul Haupt, 1997
- [15] D. Whinnett, "End User Acceptance of Security Technology for Electronic Commerce, Universität Freiburg, Deutschland 1996