

**Seminararbeit an der Fakultät für Informatik der Universität Freiburg**

**Mai 2004**

# **Überblick und Zukunftsperspektiven über gängige E-Paymentmethoden**

**Professor: A. Meier**  
**Betreuung: D. Frauchiger**

**Eliane Fischer**  
**Rte. de Givrins 16**  
**1276 Gingins**  
**eliane.fischer2@unifr.ch**

## **Abstract**

Die Übersicht der verschiedenen Bezahlverfahren lässt sich in Prepaid-, Postpaid- und Pay-Now-Verfahren gliedern. Ebenso wird kurz die Funktionsweise der Verfahren angeschnitten. Die Analyse der Erwartungen, die sowohl die Händler als auch die Kunden an den Bezahlvorgang im Internet stellen, hilft die vorgestellten Systeme auf ihre Tauglichkeit im täglichen Einsatz zu bewerten. Werden diese Kriterien eingehalten, kann das Zahlungssystem auf dem Markt bestehen. Der Vergleich gängiger Techniken prüft einige vorgestellte Systeme auf die Erfüllung der vorher erfassten Erwartungen und analysiert sie zusätzlich auf Wirtschaftlichkeit und Komplexität. Sowohl Kunde als auch Händler können hieraus ersehen, welche Verfahren für sie in Frage kommen. Das letzte Kapitel versucht anhand der aus den vorherigen Kapiteln gewonnenen Daten einen Ausblick über die zukünftige Entwicklung des E-Payment zu geben und stellt Techniken vor, die diese Entwicklungen beeinflussen werden.

**Schlüsselwörter:** E-Payment, Bezahlverfahren, E-Shop, Anforderungen, Komplexität, Wirtschaftlichkeit, Integration, Zukunftsperspektiven

## Inhaltsverzeichnis

1. Einleitung.....	2
2. E-Payment Verfahren im Überblick.....	3
2.1 Prepaidverfahren.....	3
2.1.1 Geldkarte.....	3
2.1.2 Lastschriftverfahren.....	5
2.1.3 Vorkasse.....	7
2.1.4 Prepaidkarte / MicroMoney.....	8
2.2 Postpaidverfahren.....	9
2.2.1 Kreditkartensysteme.....	9
2.2.2 net900, Telefonzahlungen.....	14
2.2.3 click & buy.....	15
2.2.4 Rechnung.....	16
2.3 Pay-Now-Verfahren.....	16
2.3.1 Nachnahme.....	16
2.3.2 Paybox / Moxmo.....	16
2.4 Alte Verfahren.....	17
2.4.1 eCash / Digitale Münzen.....	17
3. Erwartungen an E-Payment.....	18
3.1 Allgemeine Anforderungen.....	18
3.2 Erwartungen der Verbraucher.....	19
3.3 Erwartungen der Händler.....	22
4. Vergleich gängiger Techniken.....	22
4.1 Kreditkartensysteme mit SET.....	22
4.1.1 Komplexität.....	22
4.1.2 Wirtschaftlichkeit.....	23
4.1.3 Erfüllung der Anforderungen.....	24
4.2 Kreditkartenverfahren mit 3-D Secure.....	26
4.2.1 Komplexität.....	26
4.2.2 Wirtschaftlichkeit.....	26
4.2.3 Erfüllung der Anforderungen.....	26
4.2 Paybox / Moxmo.....	28
4.2.1 Komplexität.....	28
4.2.2 Wirtschaftlichkeit.....	28
4.2.3 Erfüllung der Anforderungen.....	29
4.3 Vorkasse.....	31
4.3.1 Komplexität.....	31
4.3.2 Wirtschaftlichkeit.....	31
4.3.3 Erfüllung der Anforderungen.....	32
5. Die Zukunft des E-Payment.....	34
5.1 Gibt es ein bestes Verfahren?.....	34
5.2 Chancenlose Verfahren.....	34
5.3 Zukunftsperspektiven.....	35
6. Fazit.....	35

# 1. Einleitung

Unter Electronic Payment versteht man im Allgemeinen alle Verfahren, die für das Bezahlen von Waren oder Dienstleistungen auf elektronischen Wege zur Verfügung stehen. Nach Böhle und Riehm sind E-Payment-Systeme sogar: "...spezielle Informationsverarbeitungssysteme, in denen Informationen über finanzielle Ansprüche verarbeitet werden" [Böhle, Riem 1998]. Diese Seminararbeit konzentriert sich allerdings nur auf Verfahren und Methoden, die den direkten Handel über das Internet ermöglichen. Sie soll dem Leser einen Überblick über gängige Techniken sowie eine Orientierungshilfe für die Wahl eines geeigneten System bieten. Es werden somit hauptsächlich Kunde, Händler, Banken sowie, je nach Verfahren, dritte, direkt beteiligte Instanzen betrachtet, die hier kurz vorgestellt werden. Der Kunde bestellt seine Waren über den Online-shop des Händlers. Er ist vor allem an einer schnellen, unkomplizierten und sicheren Abwicklung des Zahlvorgangs sowie einer zeitunabhängigen Möglichkeit des Einkaufens interessiert. Den Händler interessieren primär die Zahlungssicherheit und die Möglichkeit, mit dem von ihm gewählten Zahlungsmodell einen möglichst grossen Kundenkreis anzusprechen. Wird dem Kunden ein grösseres Angebot von Bezahlverfahren zur Verfügung gestellt, kann eine bessere Kundenanbindung entstehen und aufgebaut werden. Je nach E-Payment-Methode wird eine dritte Instanz, ein Zahlungsdienstleister, benötigt. Dieser leitet die Kommunikation zwischen Käufer, Anbieter und dem Payment-Gateway. Unter dem Begriff Payment-Gateway versteht man ein Autorisierungs- und Zahlungssystem, welches vom Zahlungsdienstleister zur Verfügung gestellt wird. Ebenso beteiligt an der Zahlungsabwicklung sind die Banken. Sie sind unter anderem die Ausgabestelle für Geld- und Kreditkarten. Zertifizierungsstellen, die nicht direkt am Zahlungsvorgang beteiligt sind, werden zur Verteilung von verschiedenen kryptischen Schlüsseln und Verfahren zur sicheren Datenübertragung benötigt. Des Weiteren werden die Onlinetransaktionen in Micro- und Macropaymentbereiche unterteilt, wobei Micropayment alle Transaktion bis 5,00 Euro, Macropayment alle grösseren Transaktionen umfasst. Die Verfahren an sich werden in Prepaidverfahren, Postpaidverfahren und PayNow-verfahren unterteilt. Um über die Entwicklung neuer E-Payment-Verfahren sprechen zu können, muss zunächst ein kurzer Überblick über die unterschiedlichen Methoden und deren Bevorzugung bei den Verbrauchern in Augenschein genommen werden. (Abbildung 1)

Die Abbildung zeigt deutlich, dass heutzutage immer noch die traditionellen Offlineverfahren dominieren. Die Akzeptanz neuer Onlineverfahren liegt je nach Verfahren im mittleren Bereich. Die Kunden tun sich noch schwer in diese Methoden zu vertrauen. Fehlt ihnen eine Beschreibung des Systems, können sie kein Vertrauen in die Technik entwickeln. Ist eine solche Beschreibung vorhanden, ist sie aber zu technisch gehalten, kann der Kunde wegen mangelnder Kompetenz die Sicherheit anzweifeln. Auf diese Probleme wird in Kapitel 3 „Erwartungen an E-Payment“ näher eingegangen. Als Konsequenz kann gezeigt werden, dass die Akzeptanz eines E-Payment-Verfahren stark von den Anforderungen und Erwartungen der Kunden an ein solches System abhängt. Neben der Integrität eines Systems muss auch die Wirtschaftlichkeit und die Erfüllung der Anforderungen der Kunden und Händler in Betracht gezogen werden. Dies wird in Kapitel 4: „Vergleich gängiger Techniken“ geschehen. Kapitel 5 beschäftigt sich mit den Schlussfolgerungen aus den vorherigen Kapiteln und zeigt unter anderem, dass ein allgemeingültiges Verfahren nicht existiert.

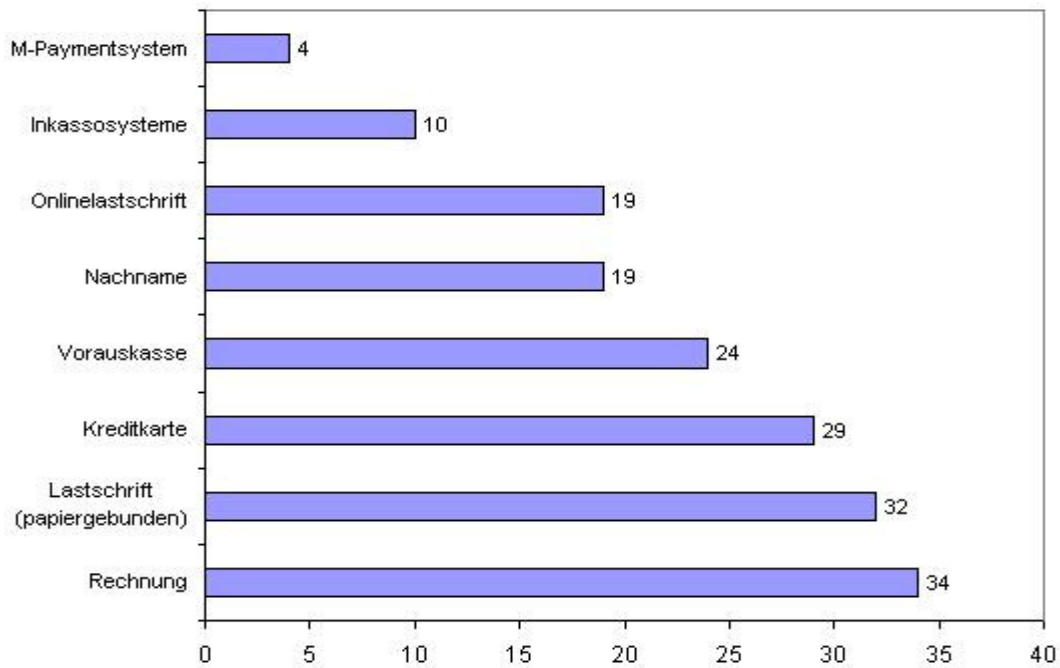


Abbildung 1: Vom Konsumenten bevorzugte Bezahlverfahren im Internet 2003  
(in %, Mehrfachnennungen möglich)  
Quelle: Institut für Wirtschaftspolitik und Wirtschaftsforschung, Universität Karlsruhe

## 2. E-Payment Verfahren im Überblick

### 2.1 Prepaidverfahren

#### 2.1.1 Geldkarte

Die Geldkarte gehört zu der Gruppe Smart-Cards. Eine Smart-Card ähnelt einer Kreditkarte, welche jedoch mit einem Prozessorchip bestückt ist. Die Geldkarte muss vor dem Gebrauch an einem Terminal einer ausgesuchten Bank aufgeladen werden. Der Begriff Aufladen bedeutet, dass die Karte entweder gegen Bargeld oder durch Abbuchen eines Girokontos mit einem Geldwert belegt wird. An der Bezahlungstransaktion sind folgende Personen oder Instanzen beteiligt:

#### Kunde

Inhaber der Geldkarte, der mit dieser die Zahlungen abschliesst.

#### Händler

Er bietet in seinem e-Shop die Zahlungsvariante Geldkarte an.

#### Kundenbank

Die Kundenbank stellt Aufladeterminale zur Verfügung und stellt sicher, dass auf die Geldkarte geladene Beträge vom Girokonto des Kunden abgebucht werden. Die Aufladedaten werden der Kartenrevidenzzentrale zur Verfügung gestellt.

#### Händlerbank

Der Händler muss einen Geldkarten-Vertrag abschliessen und erhält zu seiner Authentifizierung

eine Händlerkarte.

#### Händlervidenzzentrale

Ihre Aufgabe besteht in der Überprüfung des Zahlungsablaufes. Bei Korrektheit der Daten wird der entsprechende Rechnungsbetrag auf das Konto des Händlers gutgeschrieben.

#### Kartenevidenzzentrale

Sie verwaltet die Schattensalden. Ihr stehen die Höhe der Kartenaufloadungen und der geforderten Abbuchungen der Händler zur Verfügung. Somit dient sie als Kontrollorgan.

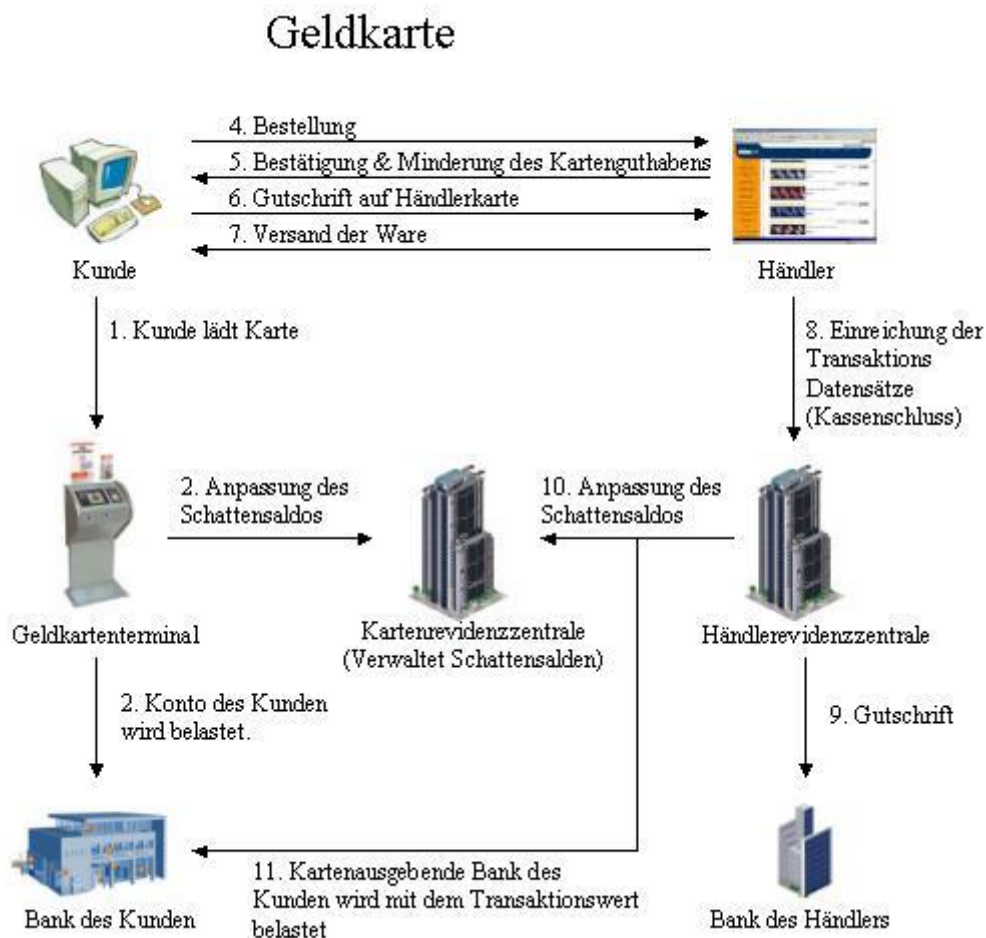


Abbildung 2: Ablaufdiagramm des Geldkartenverfahrens

#### Vorgangsbeschreibung:

Beim Aufladen der Karte durch den Kunden an einem von seiner Bank bereitgestellten Terminal wird der Aufladebetrag von seinem Girokonto abgebucht. Gleichzeitig wird in der Kartenevidenzzentrale ein Schattensaldo mit dem Aufladebetrag erstellt. Das Schattenkonto mit dem der Aufladebetrag belastet wird ist sowohl für den Kunden als auch den Händler unsichtbar. Der Kunde kann nun bei einem Onlineshop, welcher als Bezahlmethode die Geldkarte anbietet, eine Bestellung vornehmen. Nach Eingabe der Bestellung erhält der Kunde eine Zahlungsaufforderung die er bestätigen muss. Durch das Einstecken seiner Geldkarte in den CardReader werden seine Geldkartendaten sowie das Kartenguthaben an den Händler übertragen. Jegliche Kommunikation

zwischen Händler und Kunde findet SSL-verschlüsselt statt. Die Daten der Händlerkarte werden nun an den Kunden übertragen, welcher dadurch den Händler identifizieren kann. Ist der Kunde mit der Zahlung einverstanden, wird der Rechnungsbetrag von der Karte des Kunden abgebucht und es wird ein Transaktionsdatensatz beim Händler erstellt. Der Händler hat nun die Zahlungssicherheit und kann das gewünschte Produkt freigeben, beziehungsweise den Versand einleiten. Dem Kunden wird nun das neue Kartenguthaben angezeigt und es wird ein Beleg über die Transaktion bereitgestellt, welcher vom Kunden ausgedruckt werden kann. Einmal täglich macht der Händler einen „Kassenschluss“. Dabei werden die eingegangenen Transaktionsdatensätze an die Händlerevidenzzentrale gesendet. Diese gleicht das Schattensaldo der Kartenevidenzzentrale mit diesen Datensätzen ab und sorgt für eine Belastung der Kundenbank mit dem ausmachenden Betrag. Ausserdem erstellt sie eine Gutschrift des Betrages bei der Händlerbank. Für den Ablauf benötigen sowohl der Kunde als auch der Händler einige, zum Teil aufwendige, Zusatzprodukte. Eine besondere Anschaffung für den Kunden besteht im Chipkartenlesegerät. Das Chipkartenlesegerät besitzt ein eigenes Display und eine eigene Tastatur. Das eigenständige Gerät erschwert den Zugang und Angriff durch unbefugte Personen. Des Weiteren benötigt der Verbraucher eine Software, welche das Bezahlen mit Geldkarte über das Internet ermöglicht. Der Händler benötigt unter anderem ein Girokonto auf dem die Rechnungsbeträge, welche mit der Geldkarte bezahlt wurden, gutgeschrieben werden sowie einen Vertrag mit seiner Bank, von der er seine Händlerkarte erhält. Vorteile dieser Zahlungsmethode ist die teilweise Anonymität, der Händler benötigt nur die Kartenummer und den geladenen Betrag der Karte, und die erheblich hohe Sicherheit sowie die Zahlungsgarantie für den Händler vor der Auslieferung der Ware. Nachteil ist die Unsicherheit der Lieferung der Ware auf Seiten des Käufers sowie die relativ hohen Anschaffungskosten für das Kartenlesegerät.

### 2.1.2 Lastschriftverfahren

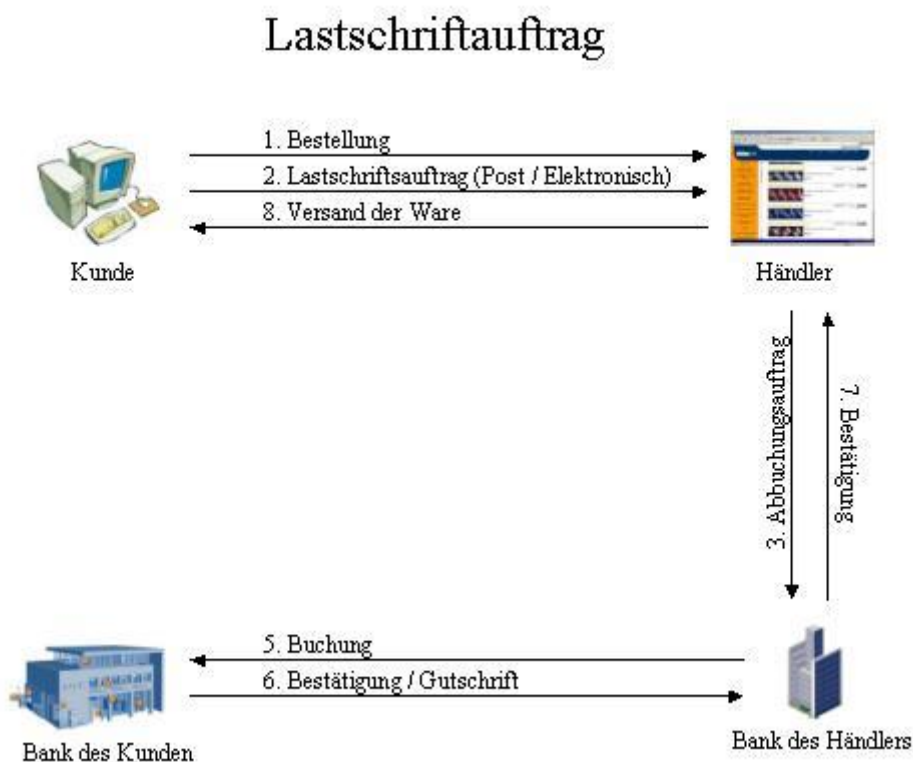


Abbildung 3: Ablaufdiagramm Lastschriftverfahren

Es existieren drei verschiedene Möglichkeiten für den Händler ein Lastschriftverfahren auf seiner Internetseite einzusetzen.

- Lastschrift durch Aufsetzen eines einfachen Formulars
- Lastschrift mit SSL-Verschlüsselung
- Lastschrift durch dritte Instanz

#### -Lastschrift mit Formular

Bei dieser Variante setzt der Händler ein einfaches Formular auf seinem Webshop.

Hat der Kunde sich entschieden, seine Rechnung per Lastschrift zu begleichen, druckt er das notwendige Formular aus und schickt es unterschrieben per Post an den Händler. Dieser kann nach Erhalt des Formulars die Lastschrift in die Wege leiten. Erst nachdem der Betrag auf dem Händlerkonto eingegangen ist, wird die Auslieferung der Ware in Gang gesetzt.

#### -Lastschrift mit SSL-Verschlüsselung

Durch die Verschlüsselung mit SSL ist es dem Verbraucher möglich das ausgefüllte Formular verschlüsselt über das Internet zu verschicken. Ebenso wird geprüft, ob es sich beim zugesandten Rechner auch wirklich um den gewünschten Kommunikationspartner, in diesem Falle um den Händler, handelt.

#### Vorgangsbeschreibung:

Nachdem der Kunde seine Bestellung losgeschickt hat, erhält er eine Nachricht, in der die Bestätigung über die Server- Authentifizierung steht. Akzeptiert der Händler die erhaltene Bestellung, steht dem Verbraucher das Lastschriftformular zur Verfügung. Sobald das Formular fertig ausgefüllt wurde wird dieses verschlüsselt an den Händler geschickt. Ist die Transaktion korrekt abgelaufen erhält der Kunde eine Bestätigung des Händlers.

Während der Händler die Lastschrift bei seiner Bank einreicht, wird die belastende Summe auf dem Kundenkonto abgebogen und auf dem Händlerkonto gutgeschrieben. Ob das Konto des Kunden genügend gedeckt ist, kann erst bei der Buchung verifiziert werden.

Wie auch beim Kreditkartenverfahren mit SSL, muss der Kunde einen SSL-fähigen Browser besitzen. Der Händler hingegen braucht neben einem SSL-fähigen Server auch ein Zertifikat zur Authentifizierung. Ein grosser Nachteil besteht in der Einzugsermächtigung. Bei dieser Variante kann diese nicht bestätigt werden, da der Kunde seine Unterschrift auf einem online-formular nicht setzen kann. Daraus folgt, dass der Kunde jederzeit die abgehobene Summe zurückverlangen kann, da es keinen gesetzlichen Hintergrund für die Gültigkeit der Abbuchungserlaubnis gibt.

#### -Lastschrift durch dritte Instanz

Für eine einzelne Bestellung ist es dem Kunden meistens zu gefährlich oder aufwendig, einen Lastschriftauftrag zu erteilen. Deswegen gibt es Drittanbieter, sozusagen Inkassounternehmen, welche dem Kunden gegenüber eine Lastschriftermächtigung besitzen. Sie kontrollieren die Daten des Kunden, die Kontodeckung und kümmern sich um das Mahnwesen. Je nach Anbieter werden dem Händler Zahlungsgarantien ausgesprochen. Beim eigentlichen Bestellvorgang muss der Kunde sich dann gegenüber dem Drittanbieter identifizieren. Dies erhöht auch die Anonymität des Kunden gegenüber dem Händler. Lastschrift durch eine dritte Instanz ist das Grundgerüst auf dem viele Paymentanbieter, zum Beispiel Moxmo, allerdings nicht als Prepaidverfahren, aufbauen.

## 2.1.3 Vorkasse

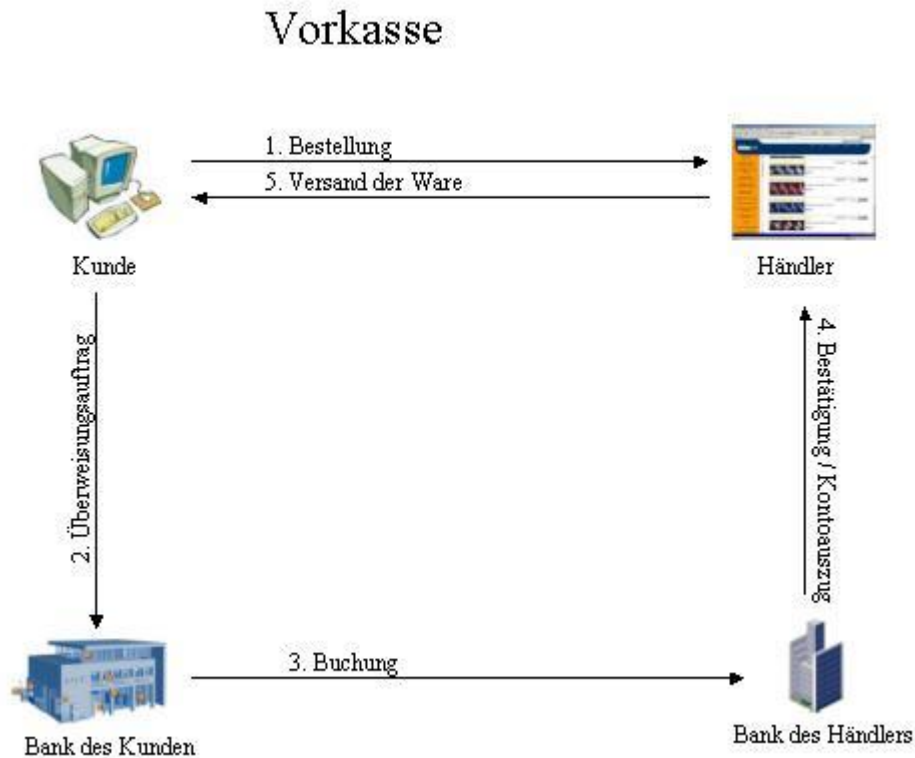


Abbildung 4: Ablaufdiagramm Vorkasse

**Verlauf der Transaktion:**

Der Kunde stellt seine Bestellung zusammen und wählt die Zahlungsvariante Vorkasse aus. Beim Kauf reeller Güter muss zusammen mit der Bestellung ebenso die Adresse angegeben werden. Diese Informationen werden über das Internet an den Händler versandt. Als nächsten Schritt muss der Händler einen Überweisungsantrag an seine Bank übermitteln. Dieser kann entweder bei der Bank abgegeben oder über online-banking vollzogen werden. Die Bank des Kunden überweist die Rechnungssumme auf das Konto des Händlers. Der Anbieter erhält auf seinem Kontoauszug die Bestätigung über den Erhalt des Rechnungsbetrages. Sobald der Händler über den Kontoauszug oder Elektronisch die Bestätigung über die Überweisung des Geldes erhalten hat, wird die Ware an den Kunden geschickt.

Vorteil dieses Verfahren ist die einfache Handhabung sowie die einfache Integration in den schon vorhandenen Webshop. Ausserdem hat der Händler eine 100%ige Zahlungssicherheit, da er die Ware erst versendet, wenn das Geld auf seinem Konto angekommen ist. Beim Kauf von nicht reellwertigen Gütern bleibt der Käufer anonym, da eine Identifizierung über den Kontoauszug nur begrenzt möglich ist. Nachteilig ist jedoch die lange Zahlungsabwicklung des Überweisungsantrages bis hin zur Bestätigung. Damit verzögert sich auch der Erhalt der Ware. Ein Spontankauf durch den Kunden ist erschwert, da dieser einen weiteren Schritt, die Überweisung, tätigen muss.

## 2.1.4 Prepaidkarte / MicroMoney

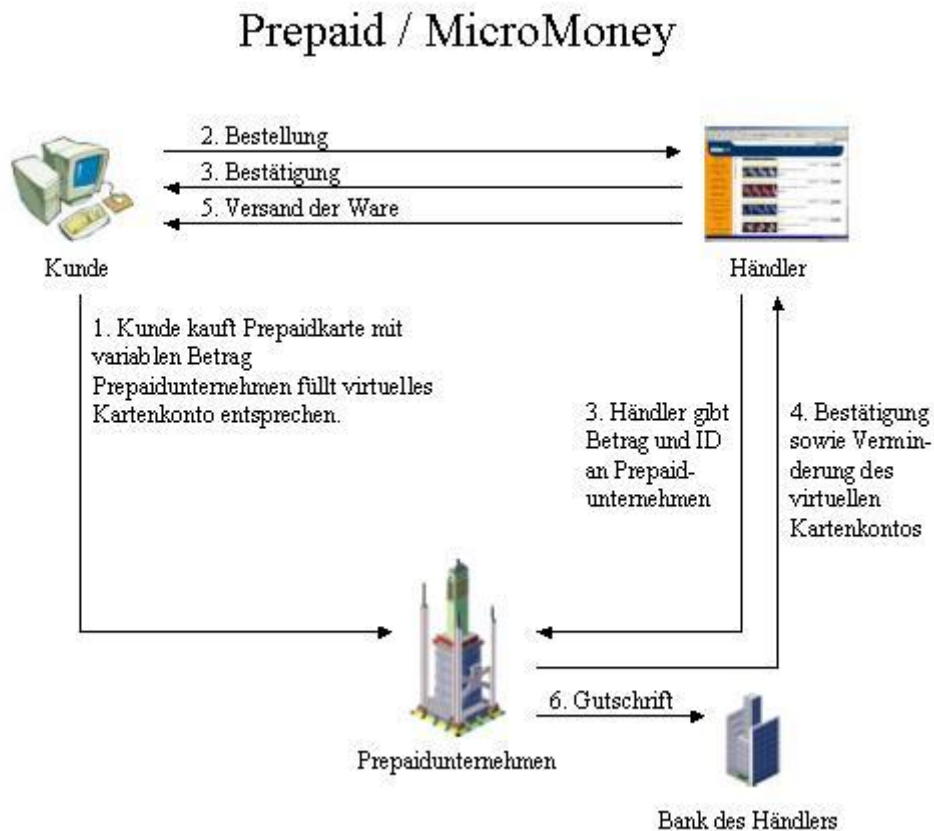


Abbildung 5: Ablaufdiagramm Prepaidverfahren / MicroMoney

## Verlauf der Transaktion:

Der Kunde kauft bei einer Prepaidunternehmung eine Prepaidkarte, welche mit einem gewünschten Betrag geladen werden kann. Zur besseren Nachvollziehbarkeit der Zu- und Abgänge wird ein virtuelles Konto bei dem Verkäufer der Karte eingerichtet. Sobald der Kunde seine Karte in Besitz hat, kann er auf den Internetseiten, die die Zahlungen mit Prepaidkarten akzeptieren, einkaufen. Hat der Käufer seine Bestellung zusammen gestellt und seine Zahlungsvariante ausgesucht, können diese Informationen an den Händler geschickt werden. Wurde die Bestellung und die Zahlungsdaten vollständig übermittelt, bekommt der Käufer eine Bestätigung zugesendet. Der Händler schickt nun den Zahlungsbetrag zusammen mit der Prepaid-ID der Karte an die Prepaidunternehmung. Diese kontrolliert die ID sowie das Kartenlimit des Kunden. Besitzt der Kunde eine für den Zahlungsbetrag ausreichend gedeckte Karte, kann eine Bestätigung der Zahlungstransaktion an den Händler geschickt werden. Das virtuelle Konto wird um die Rechnungssumme gemindert. Das Konto des Händlers wird mit der gleichen Summe gutgeschrieben. Die Ware kann nun an den Kunden ausgeliefert werden.

Der Vorteil des Verfahrens liegt in der Anonymität des Kunden gegenüber dem Händler, welcher, zumindest beim Kauf von virtuellen Gütern, nur die Kartennummer des Kunden erhält. Des Weiteren besteht für den Händler eine 100%ige Zahlungssicherheit. Nachteile für den Kunden sind die Beschränkung auf den Kartenbetrag und entstehende Zinsausfälle.

## 2.2 Postpaidverfahren

### 2.2.1 Kreditkartensysteme

Es gibt drei Varianten der Bezahlung mit Kreditkarte im Internet. Zu ihnen zählen:

- Kreditkartenzahlung mit SSL
- Kreditkartenzahlung mit SET
- Kreditkartenzahlung mit 3-D Secure

Zum besseren Verständnis werden im nächsten Abschnitt die an einer Kreditkartenzahlung beteiligten Personen vorgestellt.

#### Kunde

Der Kunde ist der Karteninhaber seiner Kreditkarte, mit welcher er im Internet bezahlt.

#### Händler

Der Händler akzeptiert die Kreditkartenzahlung und hat einen Vertrag mit der Kreditkartengesellschaft. Er besitzt eine Verbindung zum „payment gateway“ um mit der Händlerbank zu kommunizieren.

#### Kreditkartengesellschaft

Hierzu gehören unter anderem Visa, Euro- und Mastercard sowie American Express.

#### Kundenbank

Die Kundenbank, auch Issuer genannt, verteilt, mit Erlaubnis der Kreditkartengesellschaft, die Kreditkarten an die jeweiligen Kunden. Sie gibt den Händlern die Sicherheit, dass die zu bezahlende Summe verfügbar ist.

#### Händlerbank

Die Händlerbank, auch Acquirer genannt, hat die Aufgabe sich um die Verträge, Transaktionen und Betreuung der Partner zu kümmern. Die Kreditkartengesellschaften werden somit von der Händlerbank vertreten.

Für die Kreditkartenzahlung mit SET wird hier zu noch eine Zertifizierungsgesellschaft benötigt.

#### Zertifizierungsgesellschaft

Diese ist für die Authentifizierung der Beteiligten, in diesem Fall des Kunden, des Händlers und dem „payment gateway“, zuständig.

## -Kreditkartensystem mit SSL



Abbildung 6: Ablaufdiagramm des Kreditkartenverfahrens mit SSL

SSL (Secure-Socket-Layer) dient im wesentlichen zur Verschlüsselung von Internet-Formularen, die sensible Informationen beinhalten. Damit es für den Kunden nicht notwendig ist eine Bezahlung mit seiner Unterschrift zu bestätigen, muss der Händler ein MOTO-(Mail-Order/Telefon-Order)Vertrag mit der Kreditkartengesellschaft abschliessen. Somit kann der Kunde jederzeit die Abbuchung rückgängig machen und erhält den bereits abgehobenen Betrag von der Bank zurück. Da keine Zahlungsgarantie der Kreditkartengesellschaft gewährleistet wird, liegt das Geschäftsrisiko vollständig beim Händler.

Nachteil, bei der Kreditkartenzahlung mit SSL, ist das Lesen und der Missbrauch von Kreditkarten und somit deren Daten. Es ist möglich, dass Dritte Kreditkartendaten von fremden Personen bei einer Zahlung angeben. Dieses Risiko kann durch die Abfrage einer dreistelligen Prüfnummer verringert werden. Die Prüfnummer ist auf der Rückseite der Kreditkarte vermerkt. Oft wird auch das Ablaufdatum der Kreditkarte abgefragt, welches über die Kreditkartennummer validiert werden kann.

Funktionsweise einer Kreditkartenzahlung mit SSL:

Der Kommunikationsaustausch zwischen Kunden und Händler fängt mit der Bestellung und dem Zahlungswunsch des Kunden an. Dieser sucht sich gegebenenfalls seine Zahlungsvariante aus. Um sicher zu gehen, dass der Kunde auch wirklich mit dem Server des Händlers verbunden ist, bekommt er im 2. Schritt die Server-Authentifizierung. Der nächste Schritt besteht darin, die gewünschten Kreditkartendaten anzugeben. Hierzu gehören die Kreditkartennummer, Inhaber der Karte, Verfallsdatum sowie Kreditkartenart und Prüfnummer. Ebenso werden weitere sensible Daten, wie zum Beispiel Name und Adresse, angegeben. Um den Missbrauch der Daten während der Transaktion zu vermeiden werden diese mittels SSL verschlüsselt an den Händler geschickt. Der Kunde erhält eine Bestätigung des Händlers über die korrekte Übertragung der Daten. Sind die Daten beim Händler vollständig angekommen, kann die Bestellung entgegengenommen und validiert werden. Als nächster Schritt muss der Händler mit der Kreditkartenunternehmung in

Kontakt treten, um für diesen Zahlungsvorgang eine Genehmigungsnummer zu erhalten. Diese muss auf den zuvor ausgedruckten Kreditkartendaten mit der Bemerkung „Mailorder“ vermerkt werden. Die ausgedruckten Kreditkartendaten mit dem Vermerk müssen dann per Post oder Fax an die Kreditkartengesellschaft gesendet werden. Sobald dieser bei der Gesellschaft empfangen wurde, kann sie den zu bezahlenden Betrag abzüglich des Disagios auf das Konto des Händlers gutschreiben. Ebenso belastet sie mit dem gleichen Betrag das Konto des Kunden. Der Kunde benötigt für einen SSL abgesicherten Kommunikationskanal einen SSL-fähigen Internet-Browser. Zudem braucht der Händler einen SSL-fähigen Internet-Server und zur Authentifizierung des Servers ein entsprechendes Zertifikat. Das Verschicken der Kreditkartendaten für jede einzelne Bestellung ist für den Händler mit grossem Zeitaufwand verbunden. Ebenso ist die SSL-Verschlüsselung lückenhaft und kann deshalb nicht als sicherste Methode zum Versand von Daten angesehen werden. Ein SSL-Serverzertifikat muss bei einer Zertifizierungsstelle beantragt werden und ist ab 150 Euro pro Jahr erhältlich. Eine bessere, aber auch komplexere und teure Lösung, bietet das SET-Protokoll.

-Kreditkartensysteme mit SET

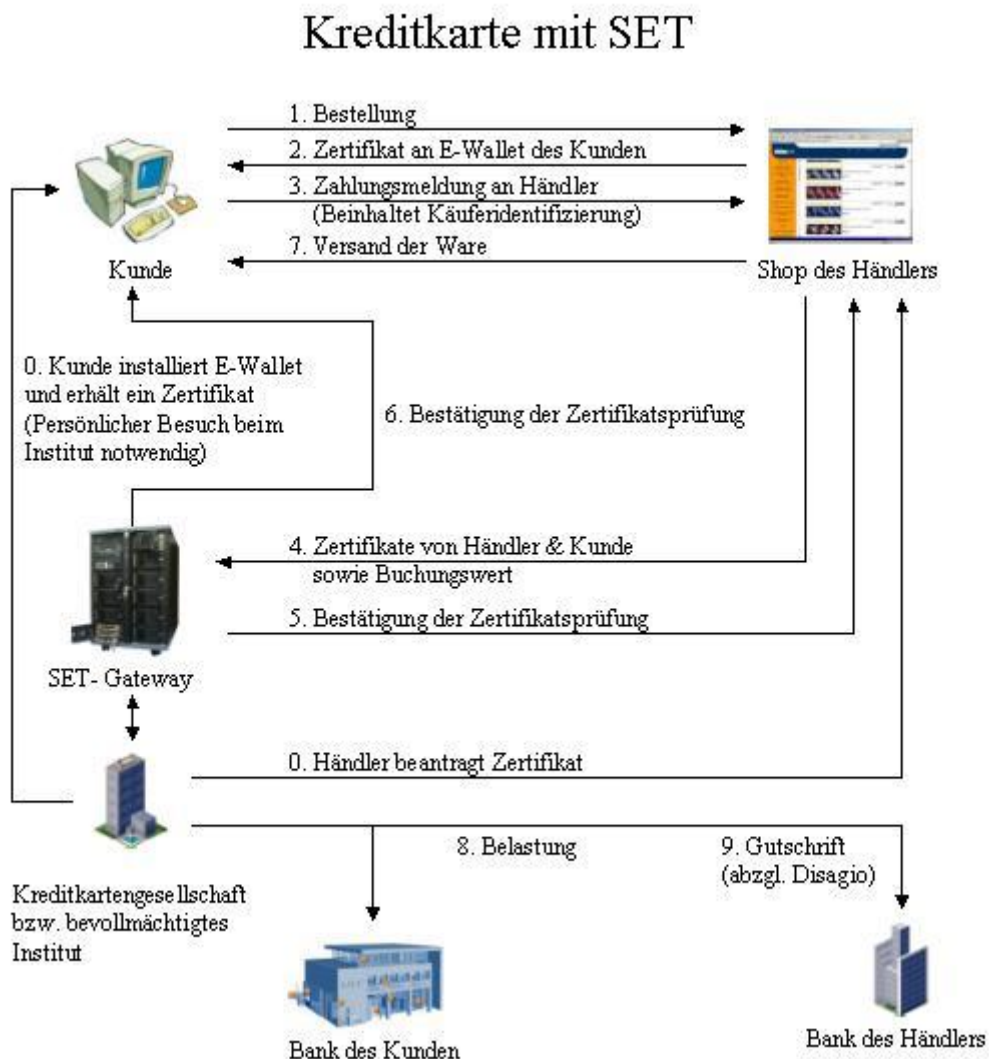


Abbildung 7: Ablaufdiagramm des Kreditkartenverfahrens mit SET

Das SET (Secure Electronic Transaction) -Protokoll ist im Gegensatz zu SSL ein reines Zahlungsprotokoll. Allerdings erhält der Händler in diesem Fall eine Zahlungsgarantie. Das Geschäft zwischen Kunden und Händler ist mit dem herkömmlichen Kartengeschäft gleichzustellen. Vorteil bringt das SET-Protokoll in der Identifikation sowohl des Händlers als auch des Kunden. Die benötigten Zertifikate werden von der Zertifizierungsstelle SETCo verteilt. Mastercard und Visa sind Unternehmen die zu dieser Instanz gehören. SET wurde unter anderem in Kooperation mit den Kreditkartengesellschaften Mastercard, Visa und den IT-Firmen IBM, Microsoft und Netscape entwickelt. Ein Vorteil liegt in der elektronischen Weiterleitung der Zahlungsinformationen zur Überprüfung.

Verlauf der Transaktion:

Um eine Transaktion über SET abzuwickeln muss der Kunde ein E-Wallet auf seinem Computer installieren und ein Zertifikat bei seinem Kreditkarteninstitut beantragen. Der Händler muss ebenfalls ein Zertifikat beantragen und eine entsprechende Software in seinen Shop integrieren. Die Transaktion zwischen Händler und Kunden läuft folgendermassen ab. Der Kunde wählt die Kreditkartenzahlungsvariante mit SET aus und schickt diese zusammen mit seinem Kaufwunsch an den Händler. Besitzt der Kunde verschiedene Kreditkarten, so kann dieser aus seinem SET-Wallet beziehungsweise seinem elektronischen Portmonnaie, welches nur durch Eingabe des persönlichen Passworts auf dem Computer zur Verfügung steht, eine Kreditkarte auswählen. Nach Erhalt des Kaufwunsches, antwortet der Händler, indem er sein Zertifikat mit Sicherheitsparametern für weitere Transaktionen an den Kunden zurückschickt. Als nächster Schritt, wird das Zertifikat des Händlers überprüft, um dem Verbraucher zu gewährleisten, dass es sich auch wirklich um den gewünschten Vertragspartner handelt. Nach der Überprüfung können die Kreditkartendaten sowie die Bestelldaten zusammen mit dem Zertifikat des Kunden an den Händler geschickt werden. Nun müssen auf Seiten des Händlers das Zertifikat und die Bestellung verglichen werden. Durch die sogenannte duale Signatur bleiben für den Händler die Kreditkartendaten verschlüsselt. Die verschlüsselten Daten müssen nun mit dem Händlerzertifikat und dem Rechnungsbetrag an das SET-Payment-Gateway geschickt werden. Das SET-Gateway kontrolliert die Zertifikate der beiden Geschäftspartner auf ihre Echtheit. Des Weiteren muss der Rechnungsbetrag des Händlers mit dem Betrag des Kaufwunsches des Kunden übereinstimmen. Daraufhin werden der Betrag sowie die Kreditkartendaten an die Kreditkartengesellschaft weitergeleitet. Die Autorisierungsstelle prüft, ob die Karte nicht gesperrt ist, das Kartenlimit nicht überschritten wird und der Händler einen Vertrag mit der entsprechenden Kreditkartenunternehmung besitzt. Die Kreditkartengesellschaft übermittelt die Autorisierung an das SET-Gateway. Dort wird die Bestätigung an den Händler weitergeleitet. In kürzester Zeit erhält der Kunde seine Zahlungsbestätigung. Der Händler kann alles zur Warenlieferung bereitstellen und erhält gleichzeitig, über die Kreditkartengesellschaft, den Rechnungsbetrag abzüglich des Disagios auf seinem Konto gutgeschrieben. Im Gegenteil hierzu wird das Konto des Kunden durch die Kreditkartengesellschaft in der Höhe des Rechnungsbetrages belastet.

Wie auch schon beim SSL-Verfahren erwähnt wurde, benötigt der Kunde einen SET-fähigen Browser. Hierzu muss ein Softwaremodul installiert werden, welches die vorher erwähnte E-Wallet auf dem Computer generiert. Dieses Wallet beinhaltet das SET-Zertifikat und die Kreditkartendaten. Im Gegenzug muss der Händler auf seinem Server die entsprechende SET-Software aufweisen. Diese Software bekommt den Kauf- und Zahlungswunsch des Kunden und gibt diese an das SET-Gateway weiter. Damit die Daten an das SET-Gateway weitergeleitet werden können, benötigt der Händler eine Online-Anbindung an dieses Gateway.

Einen weiteren komplexen Vorgang muss der Karteninhaber bei der Installation des E-Wallet vornehmen. Nachdem er eine Kreditkarte und somit eine digitale Briefftasche beantragt hat, kann der Kunde auf der Internetseite seiner Bank das für die sichere Verbindung benötigte SET-Starterkit

herunterladen und auf seinem Computer installieren um dort seine Karte eintragen zu können. Das SET Zertifikat wird bei der entsprechenden Bank vor Ort beantragt. Per Post erhält der Kunde das SET-Einmal-Passwort sowie die Internetseite auf der der Kunde sein SET Zertifikat abrufen kann. Ebenso muss der Kunde auf das Verfallsdatum seines Zertifikates achten. Diese verfällt in der Regel nach drei Jahren. Die Zertifikatsverlängerung nach Ablauf der Kreditkarte ist schwer zu handhaben. Des Weiteren dauert der Prozess bei einer gestohlenen Kreditkarte lange an. In diesem Fall muss eine neue Karte sowie ein neues Zertifikat beantragt werden. Möchte der Kunde ein neues Kartenprodukt, beispielsweise die Gold-Card, so erhält er eine neue Kreditkarte mit einem neuen Zertifikat.

Ein grosser Vorteil dieses Verfahren ist die Anonymität des Kunden gegenüber dem Händler. Der Händler erhält sofort eine Identifizierung des Kunden sowie eine Bestätigung, dass das Konto des Kunden gedeckt ist. Das Kreditkartenunternehmen gibt sogar eine Zahlungsgarantie. Als Nachteil ist für den Kunden der grosse Installationsaufwand und die Gebundenheit an den Computer auf dem das Wallet installiert ist, zu sehen. Allerdings gibt es eine neue Version der Wallet Software, welche als Java-Applet auf jedem beliebigen Rechner gestartet werden kann. Auch das Disagio, welches je nach Anbieter von 3% bis 6% variiert, ist als Nachteil zu sehen.

-Kreditkartensystem mit 3-D Secure

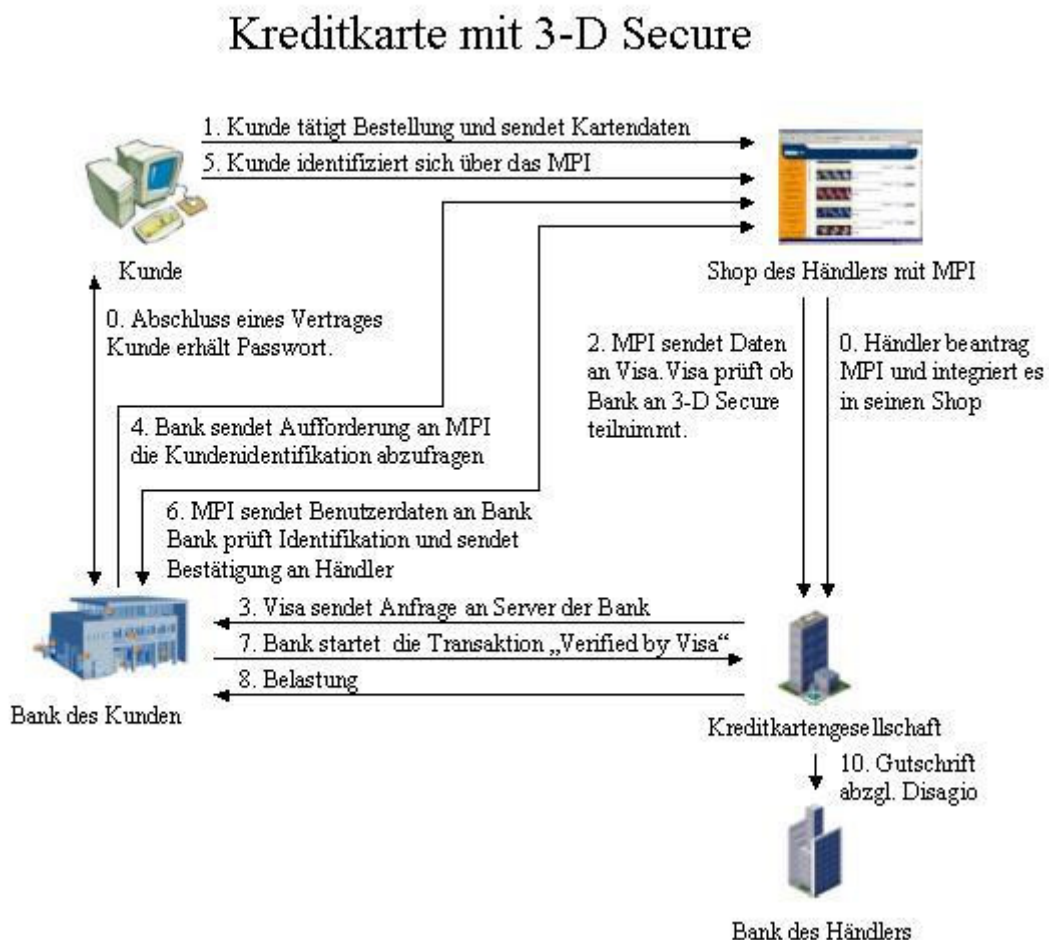


Abbildung 8: Ablaufdiagramm des Kreditkartenverfahrens mit 3-D Secure

3-D Secure (Three Domain Secure) ist eine Nachfolgeentwicklung von SET, welche von Visa und Mastercard unter den Namen „Verified by Visa“ und „Mastercard SecureCode“ angeboten wird. Mastercard ging bisher einen anderen Weg zur Authentifizierung der Teilnehmer, welche unter anderem eine Softwareinstallation beim Kunden von Nöten machte. Allerdings will sich Mastercard nun dem Verfahren von Visa angleichen und mit ihr zusammen das 3-D Secure Verfahren anbieten. Es wird deshalb hier nur die Vorgehensweise von „Verified by Visa“ aufgezeigt.

#### Vorraussetzungen

Der Kunde schliesst einen Vertrag mit der Kartenausgebenden Bank ab und erhält ein Passwort. Der Händler muss das MPI (Merchant Plugin) in seinen Webshop integrieren.

#### Verlauf der Transaktion:

Der Kunde tätigt seine Bestellung und sendet seine Kartendaten an den Händler. Das MPI sendet die Daten an Visa, wo geprüft wird ob die Kartenausgebende Bank 3-D Secure unterstützt. Ist dies der Fall wird die Anfrage an den Authentifizierungsserver der Bank weitergeleitet. Die Bank veranlasst daraufhin das MPI des Händlers eine Abfrage von User-ID und Passwort des Kunden vorzunehmen. Diese Abfrage geschieht über den Browser des Kunden. Sind die Daten korrekt, sendet die Bank eine Bestätigung an den Händler welcher dem Kunden dann auf eine entsprechende Seite leitet. Im Hintergrund wird eine normale Kreditkartentransaktion in Gang gesetzt, welche allerdings das Attribut „Verified by Visa“ trägt. Visa und Mastercard geben auf diesen Vorgang eine Zahlungsgarantie und befreien den Händler zusätzlich von den bei anderen Verfahren anfallenden „Chargeback“- Gebühren, da der Kunde die Transaktion durch Eingabe eines Passwortes bestätigt. Der Kunde hat daher nicht die Möglichkeit sich der Zahlung zu entziehen. Wie bei SET wird der Kunde vor Lieferungsausfall durch strenge Richtlinien der Zertifikatsvergabe an den Händler geschützt. Treten zu viele Forderungen seitens der Kunden an den Händler auf, verliert der Händler die Erlaubnis 3-D Secure anzubieten.

#### 2.2.2 net900, Telefonzahlungen

Dieses Prinzip erfordert, dass sowohl Kunde als auch Händler einen Vertrag mit einer dritten Instanz, in diesem Fall mit net900, besitzt. Dieses System wird vor allem beim Verkauf von elektronischen Gütern eingesetzt. Dem Verbraucher werden beim Kauf solcher Güter die Rechnungsbeträge auf einem Konto der Instanz aufaddiert und am Ende des Monats in Rechnung gestellt.

Net900 bietet zwei Zahlungsvarianten an. Entweder „Pay per Call“, bei dem für jeden Download ein bestimmter Betrag festgesetzt wird, oder „Pay per Minute“, bei der jede Minute des Downloads zum Beispiel 1 Euro in Rechnung gestellt wird.

Die ausgewählte Variante kann am Ende des Monats in Telefoneinheiten umgewandelt und mit der Telefonrechnung verrechnet werden. Dies kann über das Girokonto des Verbrauchers geschehen. Beteiligte Partner an der Zahlungskommunikation sind:

#### Kunde

Verbraucher, der eine vertragliche Abrechnungsvereinbarung mit net900 hat.

#### Händler

Der Händler besitzt ebenfalls eine vertragliche Vereinbarung mit net900 und bietet dieses Zahlungsprinzip an.

### Firma

Die Firma „in medias res“ kümmert sich um die Abrechnung von net900.

### Festnetz-, Telefonanbieter

Verbuchen gegebenenfalls die Abrechnung auf die Telefonrechnung der Kunden.

### Verlauf der Transaktion:

Möchte der Kunde gebührenpflichtige Inhalte beziehungsweise Güter erhalten, so muss er sich mit den entstehenden Kosten einverstanden erklären. Durch die erhaltene net900 Software unterbricht der Computer die Internetverbindung und wählt sich automatisch in den net900-Server ein. Auf diesem liegen entweder die elektronischen Güter bereit oder es besteht ein Link auf diese. Nun kann der Verbraucher sich die Güter herunterladen. Sobald die Güter sich auf dem Computer des Kunden befinden wird die ursprüngliche Internetverbindung wieder hergestellt. Der Kunde erhält seine net900 Abrechnung auf der Telefonrechnung seines Anbieters. Dieser muss die angefallenen Gebühren der Firma „in medias res“ zurückerstatten. Wiederum muss diese, abzüglich des Disagios, den Gewinn dem Händler gutschreiben.

Voraussetzung zur Nutzung dieses Systems ist auf Seiten des Kunden die net900 Software und eine Internetverbindung über die Telefonleitung. Besitzer eines DSL-Zugangs muss er zusätzlich ein Modem mit entsprechender Telefonleitung besitzen. Die Software veranlasst den selbstständigen Wechsel zwischen Internet- und Telefonverbindung. Auf Seiten des Händlers wird zu aller erst ein Vertrag mit der Firma „in medias res“, welche net900 anbietet, abgeschlossen. In diesem Vertrag wird festgelegt nach welcher der beiden Zahlungsvarianten abgerechnet werden soll und die entsprechenden Tarifhöhen festgesetzt. Ist der Vertrag unterschrieben, muss die betroffene Internetseite beziehungsweise das kostenpflichtige Angebot von net900 kenntlich gemacht werden. Dem Händler stehen verschiedene Möglichkeiten der Hinterlegung der elektronischen Güter zur Verfügung. Erstens, können die Güter auf dem net900-Server abgelegt werden. Zweitens bietet net900 Abstellplätze für eigene Server an oder als letzte Variante kann eine Verbindung von net900 zum eigenen Server hergestellt werden.

### 2.2.3 click & buy

Ein weiteres Verfahren ist click & buy von FIRSTGATE. Bei diesem System braucht der Käufer sich nur, durch Eingabe seiner Anschrift und seiner Konto- oder Kreditkartendaten, zu registrieren, wodurch er ein Passwort und einen Benutzernamen für seine Zahlungsvorgänge erhält. Durch seine Registrierung legt FIRSTGATE ein virtuelles Konto für den Kunden an welches in Zukunft bei Transaktionen belastet wird. Die Validierung des Kontoinhabers erfolgt über eine Überweisung von FIRSTGATE an den Kunden bei der eine PIN-Nummer angegeben wird, die wiederum bei FIRSTGATE eingetragen werden muss. Allerdings kann der Kunde schon vor der Validierung das Angebot nutzen. Der Händler stellt bei FIRSTGATE sogenannte Premium-Links ein, wobei er das Ziel des Links und einen Preis pro Aufruf angibt. Der Händler bekommt dann einen modifizierten Link von FIRSTGATE, den er in seinem Shop anbringt. Klickt der Kunde auf den Link wird er auf eine Seite von FIRSTGATE verwiesen auf der er seinen Benutzernamen und sein Passwort eingeben muss. Stimmen diese Daten mit der Anmeldung überein wird der ausmachende Betrag auf seinem virtuellen Konto abgebucht. Jeden Monat wird der gesamte Soll-Betrag des Kunden entweder durch Abbuchung von seinem Bankkonto oder mit Kreditkarte beglichen. FIRSTGATE übernimmt das Rechnungswesen und die Zahlungstransaktionen. Des Weiteren bietet die Firma Zusatzleistungen im Bereich Mahnwesen an. Vorteile dieser Methode sind einmal, dass hierfür keine Software benötigt wird und für den Kunden die Registrierung kostenlos ist. Zum anderen kann der Händler täglich seine Preise nach seinem Wunsch anpassen. Zu den grossen Kunden von

FIRSTGATE zählen unter anderem Stiftung Warentest und die Deutsche Post. Allerdings gibt der Anbieter keinerlei Zahlungsgarantien, was das Verfahren für grössere Beträge uninteressant macht.

### 2.2.4 Rechnung

Die Bezahlung per Rechnung besagt, dass der Rechnungsbetrag innerhalb einer vorgegebenen Zeitspanne auf dem Händlerkonto eingegangen sein muss. Beispielsweise 10 Tage nach Lieferung. Dieses Verfahren wird als sicheres Zahlungssystem angesehen, ist jedoch für den Händler mit einem Vorleistungsrisiko verbunden.

## 2.3 Pay-Now-Verfahren

### 2.3.1 Nachname

Die Bezahlung per Nachname bedeutet, dass bei Lieferung der Ware der ausmachende Betrag vom Transportunternehmen abgerechnet wird. Somit ist weder für den Händler noch für den Kunden mit einem Risiko zu rechnen, da die Warenübergabe mit der Bezahlung einher geht.

### 2.3.2 Paybox / Moxmo

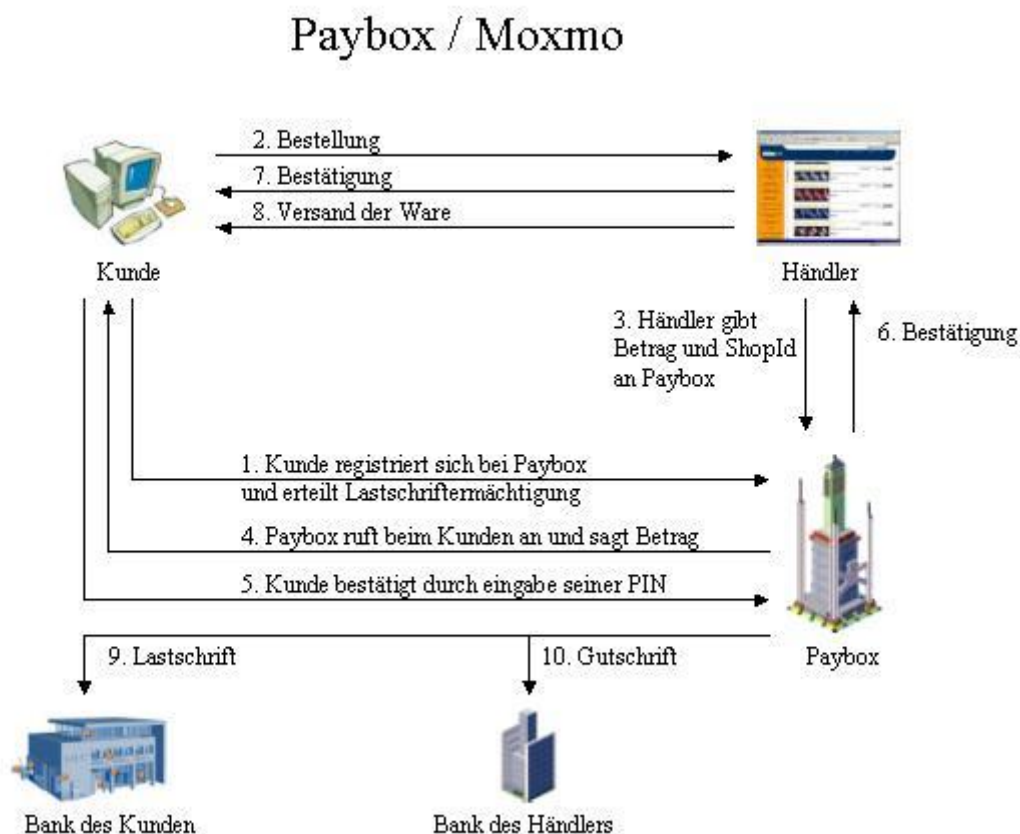


Abbildung 9: Ablaufdiagramm von Paybox / Moxmo

Bei der Transaktion sind neben dem Kunden und dem Händler noch die paybox.net AG beziehungsweise Moxmo und die Deutsche Bank AG involviert.

Nach Auswahl der Güter gibt der Käufer seine Mobiltelefonnummer ein und versendet diese Informationen an den Händler. Dieser wiederum leitet die verschlüsselten Daten an die paybox.net AG weiter. Dort werden die Daten überprüft und der Kunde wird auf seinem Mobiltelefon angerufen. Wird der Anruf vom Kunden entgegengenommen, wird diesem der Rechnungsbetrag und der Empfänger mitgeteilt. Ist der Kunde damit einverstanden wird durch eine eingegebene PIN die Zahlung bestätigt und die bevorstehende Transaktion autorisiert. Der Händler erhält von paybox die Zahlungsbestätigung worauf er dem Käufer eine Bestellungsbestätigung schickt und die Warenlieferung fertig stellt. Der Rechnungsbetrag wird mit einem Lastschriftverfahren auf dem Kundenkonto eingeholt und auf das Händlerkonto gutgeschrieben. Der Käufer braucht für diese Abwicklung ein Handy mit gültiger SIM-Karte sowie einen Vertrag mit der paybox.net AG. Der Händler muss allerdings zwei verschiedene Verträge mit paybox.net abschliessen. Einen Dienstleistungsvertrag und einen Softwarevertrag.

Moxmo bietet dem Händler zwei Systeme an. Das erste System ist das Moxmo STANDARD. Bei Moxmo STANDARD befindet sich der Kunde auf der Internetseite des Händlers. Durch eine SSL verschlüsselte Leitung wird der Zahlungsauftrag an Moxmo weitergeleitet. Sobald Moxmo diesen Zahlungsauftrag erhalten hat, führt Moxmo die Zahlungstransaktion durch und schickt eine Bestätigung an den Händler. Erhält der Anbieter diese Bestätigung muss dieser den Erhalt der Bestätigung an Moxmo wiederum bestätigen. Bei diesem System bleibt der Kunde während der ganzen Zahlungstransaktion auf der Website des Händlers.

Das zweite System heisst Moxmo LITE. Bei diesem System wird der Kunde von der Internetseite des Händlers auf die Seite von Moxmo weitergeleitet. Dort trägt der Kunde in einem SSL sicheren Formular seine Mobiltelefonnummer ein. Daraufhin kann Moxmo die Zahlungstransaktion durch Bestätigung der Moxmo-PIN durchführen. Nach dieser Zahlungsabwicklung wird der Kunde wieder auf die Händlerseite weitergeleitet.

## 2.4 Alte Verfahren

### 2.4.1 eCash / Digitale Münzen

Digitale Münzen sind dem echten Geld gleichzusetzen. Der Unterschied ist, dass die Kunden eine digitale Werteinheit besitzen, die als binäre Datei bereitsteht. Erhältlich sind digitale Münzen bei Banken. Sie werden vom Girokonto direkt auf den Computer in einem elektronischen Geldbeutel geladen. Der Händler kann also ganz einfach die Münzen bei seiner Bank auf sein Konto gutschreiben.

Neben dem Kunden und dem Händler wird für die Zahlungsabwicklung eine eCash-Bank benötigt. Ihre Aufgabe ist es digitale Münzen auszugeben, auf ihre Echtheit zu prüfen und sie gegen echtes Geld einzutauschen.

Verlauf der Transaktion:

Durch die Bestellung und dem somit getätigten Zahlungswunsch erhält der Kunde eine Aufforderung zum Zahlen. Akzeptiert der Verbraucher diese, schickt er dem Händler den Forderungsbetrag in digitaler Währung. Zur Überprüfung der digitalen Münzen sendet der Händler diese an die eCash-Bank. Sobald die Überprüfung vollendet wurde, wird der Betrag auf das eCash-Konto des Händlers aufaddiert und er erhält hierüber eine Bestätigung. Mit dem Erhalt der Bestätigung kann die Warenauslieferung beginnen. Die Summe des eCash-Kontos kann auf das Girokonto des Händlers überwiesen werden. Damit der Zahlungsablauf durchgeführt werden kann, muss der Verbraucher ein eCash-Konto und eine geeignete Software besitzen. Genauso benötigt der

Händler ein eCash-Konto und eine entsprechende eCash-Händler-Software.

Vorteil dieses Zahlungssystems ist die Anonymität des Kunden. Jedoch wurde eCash von vielen als zu kompliziert in der Handhabung bewertet.

### 3. Erwartungen an E-Payment

#### 3.1 Allgemeine Anforderungen

Jedes Zahlungssystem muss sich an bestimmte Anforderungen halten, um auf dem elektronischen Markt bestehen zu können. Hilfreich sind die folgenden allgemeinen Anforderungen nicht nur für schon bestehende sondern auch für zukünftige E-Payment-Verfahren. Die ersten vier Anforderungskriterien sind bekannt unter dem Kürzel ACID, welcher sich aus den Anfangsbuchstaben der einzelnen Anforderungspunkte zusammensetzt.

##### Atomicity (Totalität, Unteilbarkeit)

Es muss gewährleistet sein, dass die Zahlungstransaktion vollständig abläuft und gegebenenfalls bei einem Abbruch der Datenübermittlung storniert wird. Wird die Übermittlung unterbrochen so kann dies zu unvollständigen oder sogar zu falschen Informationen führen, beispielsweise einer falschen Rechnungssumme.

##### Consistency (Konsistenz)

Kunde und Händler, beziehungsweise die an der Transaktion beteiligten Personen und Instanzen, müssen über alle notwendigen Daten der Bezahlung in Kenntnis gesetzt werden. Insbesondere über die Höhe, Zeitpunkt und Zweck der Transaktion. Dies bedeutet allerdings, dass nicht unbedingt alle beteiligten Parteien alle Transaktionsdaten kennen, sondern nur beschränkten Zugriff haben. Bei manchen Verfahren kennt der Händler nur die Bestellung sowie die Adresse des Kunden zur Auslieferung der Ware. Hingegen ist die Kreditkartengesellschaft nur in der Lage die Zahlungsdaten zu lesen. In der Konsistenz mitinbegriffen ist die Integrität, welche gewährleistet, dass die Informationen und Daten der Zahlung nicht von aussenstehenden Personen eingesehen und manipuliert werden können. Somit darf es nur den beteiligten Personen gestattet sein und ermöglicht werden in diese Daten Einblick zu haben. Das Vertrauen kann somit bestärkt werden.

##### Independence (Unabhängigkeit)

Unterschiedliche Zahlungssysteme sollten sich bei ihrer Ausführung nicht gegenseitig behindern. Die einzelnen Verfahren müssen gleichzeitig benutzbar und zeitunabhängig sein.

##### Durability (Dauerhaftigkeit)

Bei einem Ausfall der Systeme muss gewährleistet sein, dass die letzte Transaktion beziehungsweise die letzte Ausführung wieder hergestellt oder nachzuvollziehen ist. Nützlich ist dies bei Zahlungsverfahren bei denen erforderliche Dateien auf dem Rechner gespeichert sind. Dies trifft zum Beispiel bei digitalen Brieftaschen oder digitalen Münzen ein. Um eine vollständige Wiederherstellung zu gewährleisten sollten zur Vorbeugung regelmäßige Backups gemacht werden.

Weitere allgemeine Erwartungen sind:

##### Internationalität

Können Käufer Güter aus dem Ausland beziehen und Händler ebenso Zahlungen aus anderen

Ländern empfangen, ist das Zahlungsverfahren international anerkannt und etabliert. Dies kann als Anhaltspunkt einer weit verbreiteten und akzeptierten Methoden gesehen werden. Hierfür muss der Händler jedoch ein Verfahren finden, welches unterschiedliche Währungen und Zahlungsabläufe unterstützt.

#### Verlässlichkeit

Nicht nur die Kunden sondern auch die Händler sind abhängig davon, wie gut und zuverlässig die Provider der Bezahlverfahren arbeiten. Bei Kreditkartenunternehmen und Banken wird die Arbeit häufig als zuverlässig eingestuft, da diese schon länger in diesem Bereich und in dieser Branche arbeiten und einen Ruf besitzen. Hingegen rufen kleine und unnamhafte Unternehmen ein grösseres Risiko hervor.

#### Kosten

Fast alle E-Payment Verfahren verursachen Kosten. Betreffen die Kosten direkte den Kunden, kann dies die Entscheidung das entsprechende Verfahren zu verwenden, negativ beeinflussen. Der Händler muss sich entscheiden, ob er die Kosten auf den Kunden abwälzt oder sie selbst trägt. In beiden Fällen muss er auf seine Wettbewerbsfähigkeit achten. Die Kosten entscheiden, neben der Komplexität des Verfahrens, welche Beträge über das E-Paymentsystem abgerechnet werden können.

Eine Übersicht der Kosten gängiger Verfahren ist in Kapitel 4 unter „Wirtschaftlichkeit“ zu finden.

### 3.2 Erwartungen der Verbraucher

#### Sicherheit vor Datenmissbrauch

Heutzutage stellen Kundendaten einen nicht zu unterschätzenden Wert dar.

Es existieren bereits Unternehmen die sich nur durch das Sammeln von Kundendaten, auch Profile genannt, finanzieren. Die Beschaffung dieser Daten verläuft nicht ausschliesslich mit der Zustimmung des Kunden. Bestes Beispiel ist das sogenannte „Phishing“ bei dem sich Trickbetrüger in E-Mails als Firmen ausgeben um an das Passwort oder Profildaten ihres Opfers zu kommen. Im Zusammenhang mit E-Payment bezieht sich der Datendiebstahl entweder auf das Abfangen der Kundendaten beim Bestell- und / oder Authentifizierungsvorgang oder auf den Einbruch in den Server des Händlers, um an die gewünschten Kundendaten zu kommen. Die beste Möglichkeit, sich vor Datendiebstahl zu schützen, ist es keine Daten, die über die Bedürfnisse der Transaktion hinausgehen, abzufragen. Ausserdem besteht die Möglichkeit eine dritte Instanz zur Abwicklung der Zahlungstransaktion einzubinden, so dass der Händler beispielsweise nur eine Identifikationsnummer des Kunden erhält. Diese Instanz kümmert sich dann um die Validierung der Kundendaten. Dieses Verfahren wird zum Beispiel bei Kreditkartensystemen mit SET eingesetzt. Dies steht in Konkurrenz zu der Händlererwartung, Daten über den Kunden zu erhalten. Der Datendiebstahl kann auch eine Vorarbeit zum Datenmissbrauch darstellen, zum Beispiel wenn es sich um Konto- oder Kreditkartendaten handelt. Eine Verschlüsselung der Daten sowie eine Authentifizierung der Transaktionsteilnehmer kann das Risiko des Datendiebstahls minimieren. SSL und andere Zertifizierungsverfahren bieten durch Verschlüsselung und Zertifizierung beide Möglichkeiten an. Je nach Land existieren auch Gesetze gegen die Weiterveräußerung von Daten, wobei diese durch die Globalität des Internet leicht umgangen werden können.

Der Datenmissbrauch ist der Vorgang die, illegal, angeeigneten Daten für Betrugszwecke zu verwenden. Bekanntestes Beispiel ist der Kreditkartenbetrug durch Angabe einer fremden Kreditkartennummer und deren Prüfsummen. Aber auch Pins und Passwörter können

verwendet werden um auf fremde Rechnung einzukaufen. Meist reicht es nicht aus den elektronischen Angriff, zum Beispiel durch Abhören der Transaktionsdaten, zu verhindern. Auch der Kunde muss auf die Wichtigkeit seiner persönlichen Daten sensibilisiert werden. Manche Anbieter geben dem Kunden die Möglichkeit einen Überblick über die auf seinen Namen getätigten Transaktionen zu erhalten. Damit besitzt der Kunde ein Kontrollinstrument um sich unabhängig von den Sicherheitsvorkehrungen der Bezahlsystemanbieter vor Missbrauch zu schützen. Zum Beispiel bietet FIRSTGATE seinen Kunden eine Seite an, auf der tägliche sämtliche vollzogenen Transaktionen aufgeschlüsselt werden. Natürlich hat der Anbieter von E-Paymentssystemen einen Einfluss auf die Sicherheit des Systems. Länge und Zusammensetzung von Passwörtern, aufeinander aufbauende Sicherheitssysteme, zum Beispiel Kreditkartennummern und Prüfsummen, sowie die Verhinderung von physikalischen Angriffen, beispielsweise wenn wenig Kommunikation über offene Netze durchgeführt werden, mindern das Risiko des Datenmissbrauchs. Der Kunde, welcher meist nicht über das technische Know-How verfügt, ein System als sicher oder unsicher zu bewerten, möchte die Sicherheit, dass ein entstandener Schaden ohne viel Aufwand rückgängig gemacht werden kann.

#### Sicherheit vor Betrug

Meist hat der Kunde beim Onlinekauf keinen physikalischen Kontakt zum Händler. Es ist ihm nur mit Aufwand möglich, die Korrektheit der Händlerdaten zu überprüfen. Bei Prepaidverfahren besteht für den Kunden demnach immer die Gefahr die bestellte und bezahlte Ware nicht zu erhalten. Deswegen wünscht sich der Kunde die Möglichkeit seine Zahlungsaufträge zu stornieren oder eine Kontrollinstanz zwischenschalten, die die Zahlung an den Händler erst beim Erhalt der Ware einleitet. Dies steht in Konkurrenz zur Zahlungssicherheit des Händlers, da viele Stornierungsmechanismen auch verwendet werden können um die Bezahlung von bereits erhaltener Ware rückgängig zu machen.

#### Benutzerfreundlichkeit / Komplexität

Der Kunde wünscht sich ein unkompliziertes Bezahlverfahren das weder viel Zeit noch eine hohe Einarbeitung benötigt. Zum einen gibt es einen fixen Aufwand, also einmalige Anstrengung, zum Beispiel Hardware- oder Softwareinstallationen, Registrierungen und die Einstellung digitaler Zertifikate. Zum anderen fällt auch ein variabler Aufwand an. Bei jeder Zahlung müssen die persönlichen Daten oder Passwörter und PIN-Nummern angegeben werden.

Um einen Spontankauf zu ermöglichen darf das System keine Vorleistungen erwarten.

Optimal wäre ein System, welches dem Kunden zeit- und ortsunabhängig die Möglichkeit gibt seine Waren zu bestellen. Bei den meisten Bezahlverfahren steht dies allerdings im Widerspruch zur eindeutigen Identifizierung des Kunden. Durch die technisch bedingte Anonymität des Internet ist eine persönliche Identifizierung des Kunden vor der ersten Transaktion von Nöten. Eine Ausnahme bilden die Prepaidverfahren, bei denen die Zahlungssicherheit für den Händler maximiert wird, wodurch auf eine Identifikation des Kunden verzichtet werden kann.

Ein weiterer wichtiger Punkt ist die Komplexität des Anmeldeverfahrens im Bezug auf zu installierende Software oder Hardware. Viele Kunden sind mit der Installation von Software, Hardware oder Zertifikaten überfordert und können dies nicht ohne Hilfe von Dritten tun.

Sind neben dem Händler und dem Kunden noch Dritte an der Transaktion beteiligt, muss es dem Kunden klar sein, an wen er sich im Falle einer Störung zu wenden hat.

#### Portabilität

Die Portabilität eines Verfahrens oder eines Systems wird von noch nicht vielen als nötig angesehen. Unter Portabilität versteht man plattformunabhängige Programme. Sozusagen Software, die auf unterschiedlichen Computern läuft, selbst wenn diese verschiedenen Betriebssysteme nutzen.

Für die internationale Ausbreitung von Bezahlssystemen ist die Portabilität sinnvoll und von Nöten. Wird Portabilität erwartet, so fallen alle Systeme, welche den Einsatz von digitalen Zertifikaten beinhalten, weg. Auch an Hardware gebundene Verfahren wie die Geldkarte stören die Portabilität. Möglich wäre es diese, von einem Computer zum anderen zu wechseln, jedoch ist dies mit hohem Aufwand und einem gewissen Know-How des Benutzers verbunden. Zu den geeigneten Verfahren gehören alle M-Payment-Systeme, da diese Computerunabhängig getätigt werden können. Ebenso gehören hierzu die herkömmlichen Verfahren, wie beispielsweise das Bezahlen per Rechnung oder per Nachname.

#### Kosten

Verlangt ein Bezahlverfahren eine Anmeldung die mit Kosten verbunden ist, muss der Kunde sicher sein, dass es sich um eine lohnende Investition handelt. Gerade bei unbekanntem und neuen Verfahren kann es dem Kunden passieren, dass er hohe Anmeldegebühren zahlt aber später keinen Nutzen aus dem Verfahren ziehen kann, beispielsweise weil nur wenige Händler das Verfahren anbieten. Möchte der Kunde nur einen Spontankauf tätigen scheut er sich meist vor hohen Registrierungsgebühren, da er keine weitere Nutzung des Verfahrens plant. Bei Prepaidverfahren sind auch die entstehenden Zinsausfälle zu berücksichtigen. Neben den Anmeldegebühren sind auch Anschaffungskosten für Hardware, zum Beispiel das Chipkartenlesegerät beim Geldkartenverfahren, zu berücksichtigen. Gerade bei kleinen Rechnungsbeträgen lehnt der Kunde es ab hohe Transaktionsgebühren zu bezahlen. Bei den meisten Verfahren ist entweder die Anmeldegebühr oder die Transaktionsgebühr hoch, was den Kunden zwingt sein Kaufverhalten bei der Entscheidung für ein Bezahlverfahren festzulegen.

#### Anonymität

Viele Kunden ziehen den Einkauf über das Internet dem Realkauf wegen der Anonymität vor. Allerdings machen viele Bezahlverfahren dieses Kriterium zunichte, da sie zum Beispiel persönliche Kundendaten wie Rechnungsadresse benötigen. Auch die Angst vor Datendiebstahl oder Missbrauch stärken das Verlangen des Kunden nach einer Anonymen Transaktion. Beim Kauf von virtuellen Gütern, wie zum Beispiel E-Books oder dem Download von Musikstücken, kann eine 100%ige Anonymität des Kunden erreicht werden, wenn das Bezahlverfahren dem gerecht wird. In diesen Fällen kann eine dritte Instanz die Anonymität des Kunden gegenüber dem Händler ermöglichen. Hier ist zum Beispiel das SET-Protokoll zu nennen. Bei realen Gütern gibt es wegen der benötigten Postadresse noch kein Verfahren, welches eine Anonymität des Kunden gewährleistet.

#### Image

Die Anmeldung bei einem Bezahlverfahren macht, gerade wenn sie mit hohen Kosten verbunden ist, nur Sinn wenn der Kunde sicher sein kann dieses bei vielen verschiedenen Händlern anwenden zu können. Bei der Wahl des Bezahlverfahrens spielt das Image deswegen eine grosse Rolle. Ein weiterer wichtiger Punkt ist die Zukunftssicherheit des Verfahrens. Wenn der Kunde sich nicht sicher ist, dass das Verfahren über einen gewissen Zeitraum existiert, wird er sich für ein anderes Verfahren entscheiden.

#### Weitere Dienstleistungen

Zusatzleistungen sind zwar keine Anforderungen oder Erwartungen an ein E-Payment-System, jedoch können diese die Akzeptanz solcher Verfahren erhöhen. Beispielsweise bietet Paybox an, Überweisungen auf andere Konten über das Handy zu tätigen, die über das Mobiltelefon bestätigt werden. Ein weiteres Verfahren namens Street Cash kann man neben der Bezahlfunktion auch sogenannte virtuelle Tickets, zum Beispiel Theater- oder Kinokarten, die in Form von einer SMS

auf das Mobiltelefon geschickt werden, kaufen.

### 3.3 Erwartungen der Händler

#### Sicherheit vor Betrug

Die Sicherheit vor Zahlungsausfall stellt den grössten Erwartungsfaktor des Händlers dar. Durch die Wahl eines geeigneten Zahlungsverfahrens kann er dieses Risiko jedoch einschränken.

Hierzu zählen beispielsweise die Prepaidverfahren oder die Pay-Now-Verfahren.

Auch bieten manche Payment Provider eine Zahlungsgarantie auf Ihre Bezahlsysteme. Der Händler ist verpflichtet, die von ihm verwendeten persönlichen Daten gegen Zugriffe von Unbefugten zu schützen. Dadurch entstehen für ihn Kosten und Aufwand. Doch auch wenn der Händler die Kunden- und Transaktionsdaten outsourced ist es für ihn immer noch eine Frage des Images, wenn das von ihm gewählte Verfahren fehlerhaft ist und es zum Missbrauch von Kundendaten kommt. Viele bevorzugen eine eigenständige Verwaltung der Kundendaten sowohl aus Sicherheitsgründen wie auch aus Gründen des Customer Relationship Management.

#### Kosten

Je nach Bezahlmethode entstehen unterschiedliche Installationskosten oder Einrichtungsgebühren. Wenn auf ein Outsourcing verzichtet wird, müssen Mitarbeiter eventuell geschult oder neu eingestellt werden. Je nach Verbreitung des Verfahrens möchte sich der Händler nicht an grosse Investitionen binden. Aus diesem Grund sollte auch die Integration des Bezahlverfahrens in den bestehenden Shop nicht zu aufwendig sein.

Die im laufenden Betrieb anfallenden Kosten lassen sich unterteilen in Gebühren und Transaktionsbeteiligungen. So stellen zum Beispiel Zertifikate, die ständig erneuert werden müssen, eine Gebühr dar, während das Disagio der Kreditkartenunternehmen eine Transaktionsbeteiligung ist. Je nach Preis der angebotenen Ware oder Dienstleistung ist für den Händler das eine oder das andere sinnvoll. Der Händler möchte ausserdem eine gewisse Stabilität der Kosten, damit er diese in seine Preiskalkulation mit einbeziehen kann.

#### Image

Durch die Kosten eines Bezahlsystems muss sich der Händler darauf verlassen können, dass es ihm einen Wettbewerbsvorteil verschafft. Paymentssysteme die eine Anmeldung des Kunden benötigen, sind darauf angewiesen eine hohe Verbreitung zu besitzen, damit der Händler eine hohe Anzahl der potentiellen Kunden ansprechen kann. Um diesen Faktor einschätzen zu können, verlangen viele Händler eine unkomplizierte Handhabung des Paymentsystems für den Kunden.

#### Weitere Dienstleistungen

Je nach Art der angebotenen Ware oder Dienstleistung kann es sinnvoll sein, weitere Teile des Inkassowesens, wie zum Beispiel das Rechnungs- und Mahnwesen, an den Paymentanbieter abzugeben.

## 4. Vergleich gängiger Techniken

### 4.1 Kreditkartenverfahren mit SET

#### 4.1.1 Komplexität

Aufgrund seiner Komplexität ist das Kreditkartensystem mit SET schwer verständlich und kann deshalb nicht schnell und einfach installiert und gleich daraufhin benutzt werden. Die Händler benötigen auf jeden Fall einen SET fähigen Server. SET ist ein offenes Protokoll, was es dem Händler ermöglicht eine eigene Implementierung in seinen Shop vorzunehmen, beziehungsweise eine Drittfirma mit der Implementierung zu beauftragen. Damit der Händler das Verfahren in seinen Shop integrieren kann, benötigt er einen Kreditkartenakzeptanzvertrag. Dieser Vertrag kann bei der entsprechenden Händlerbank, dem Acquirer, eingeholt werden. Beispiele für einen Acquirer sind Citicorp Kartenservice von der Citibank und American Express. Der Händler erhält dann eine Vertrags-Unternehmer-Nummer, auch VU-Nummer genannt. Mit Hilfe der VU-Nummer kann mit einem Payment Provider in Kontakt treten. Dieser kümmert sich um die Verbindung zwischen dem e-Shop und dem Payment-Gateway der Händlerbank. Ebenfalls übernimmt der Provider die Abrechnung mit den Kunden. Kommt es bei einem Kunden zu einem Rücktritt der Zahlungstransaktion, so wird durch den Acquirer eine Gutschrift auf dem Kundenkonto durchgeführt. Neben der Rückbelastung werden dem Händler zusätzliche Gebühren in Rechnung gestellt. Die Acquirer setzen ein Limit für die Rückbelastungsquote. Übersteigt diese 2% wird die VU-Nummer gekündigt. Anstelle der festgelegten Rückbelastungsquote kann auch das Disagio aus Risikogründen erhöht werden. Die Komplexität auf Kundenseite ist sehr hoch, was die meisten Kunden abschreckt dieses Verfahren zu benutzen. Neben einer eindeutigen Identifizierung bei dem entsprechenden Kreditkarteninstitut benötigt der Kunde die Walletsoftware, welche er nicht nur installieren sondern auch auf seine Kreditkarten konfigurieren muss. Die Verwendung von SET auf mehreren Computern oder Mobilgeräten erweist sich als schwer.

#### 4.1.2 Wirtschaftlichkeit

Die laufenden Kosten, beziehungsweise das Disagio, werden jährlich errechnet und liegen zwischen 3% und 6% des Umsatzes. Ausserdem muss für die Vertrags-Unternehmer-Nummer eine Servicegebühr gezahlt werden. Entscheidet der Händler sich für eine eigene Integration des SET-Protokolls kann er laut einem Bericht von Visa Deutschland 1998 mit Kosten von 15.000 DM bis 20.000 DM für die Softwareentwicklung rechnen. Eine Alternative ist das Outsourcing der Transaktionsabwicklung an einen Paymentprovider. Beispiele für Payment Provider sind Avicom ([www.avicom.de](http://www.avicom.de)) und Webtrade.net ([www.webtrade.net](http://www.webtrade.net)). Allerdings fallen dem Händler dann weitere Gebühren an.

Beispiel für eine Gebührenaufstellung von Webtrade.net und Avicom:

	<i>Webtrade.net</i>	<i>Avicom</i>
Einrichtungsgebühr	19,90 €	199,00 €
Monatliche Gebühr	19,90 €	49,00 €
Transaktionskosten	0,49 €	0,89 €
Mindestlaufzeit	1 Monat	12 Monate

Je nach Payment Provider variieren auch die Kosten. Der Händler sollte daher vor der Auswahl des Payment Providers die Kosten der einzelnen Anbieter vergleichen. Ebenso sollte der Händler die Angebote in Voraussicht mit seinem elektronischen Shop abstimmen. Die unterschiedlichen Laufzeiten sollten berücksichtigt werden. Je kürzer die Laufzeit beträgt desto schneller kann das System gekündigt und somit aus dem Shop entfernt werden. Zu beachten sind die Gebühren pro Transaktion, da diese schnell in die Höhe wachsen können und gegenüber der monatlichen Gebühr sich nicht mehr lohnen würden.

#### 4.1.3 Erfüllung der Anforderungen

##### -Erfüllung der allgemeinen Forderungen

###### Atomicity

Die Sicherheit der Transaktion ist gegeben, da der ganze Vorgang in Echtzeit abläuft und der Händler eine Bestätigung erhält, wenn die Daten beim Kreditkartenunternehmen angelangt sind. Dieses muss sich durch regelmässige Backups vor Datenverlust schützen.

###### Consistency

Die beteiligten Parteien bekommen ihre jeweils notwendigen Daten zugeschickt. Da das Kreditkartenunternehmen bzw. der SET-Gateway als dritte Instanz fungiert, werden nur die notwendigsten Daten an den Händler geschickt. Der Missbrauch der Daten durch Unbefugte ist so gut wie ausgeschlossen, da jede Datenübertragung innerhalb des SET-Protokolls 1024 bit RSA verschlüsselt ist.

###### Independence

Das Wallet ist eine eigenständige Software die andere Bezahlssysteme nicht beeinflusst. Auf der Seite des Händlers können andere Bezahlssysteme angeboten werden. Gerade SET-Light (einem Service des Anbieters SET4U), also das Auslagern von SET auf einen anderen Webserver, macht es dem Händler leicht verschiedene Bezahlssysteme zusammen mit SET anzubieten.

###### Durability

Wie bei Atomicity bereits erwähnt liegt durch die sofortige Datenübermittlung an den SET-Gateway die Sicherungspflicht beim Betreiber des Gateways. Es ist anzunehmen, dass diese Daten ausreichend gesichert werden.

###### Internationalität

Das SET-Verfahren profitiert von der Internationalität der verwendeten Kreditkarte. Allerdings gibt es ausserhalb Europas kaum Händler, die eine Zahlung per SET anbieten.

###### Verlässlichkeit

Über die Verlässlichkeit von SET können keine eindeutigen Aussagen getroffen werden, allerdings besitzen die anbietenden Kreditkartenunternehmen einen guten Ruf.

##### -Erfüllung der Anforderungen der Kunden

###### Sicherheit vor Datenmissbrauch

Durch das SET-Protokoll ist dem Kunden eine hohe Sicherheit geboten. Die Übertragung der Daten wird durch einen starken 1024 bit Algorithmus verschlüsselt, um den Angriff dritter Personen zu

vermeiden. Durch die Struktur von SET erhält der Händler nur sehr wenige Daten über den Kunden, was die Sicherheit vor Datenmissbrauch weiter erhöht.

#### Sicherheit vor Betrug

Sowohl Händler als auch Kunde werden durch ihre Zertifikate identifiziert. Die Kreditkartenunternehmen bieten eine Zahlungsgarantie auf die SET- Transaktionen. Da ein Händler nach einer gewissen Anzahl von Rücküberweisungen sein SET-Zertifikat verliert, kann der Kunde davon ausgehen, dass ein SET zertifizierter Händler vertrauenswürdig ist. Trotz der Zahlungsgarantie bleibt dem Kunden die Möglichkeit der Rückforderung.

#### Benutzerfreundlichkeit

Das Ausfüllen des Formulars mit Name, Adresse, Kreditkartenart, Kreditkarteninhaber, Gültigkeitsdatum der Kreditkarte und der Kreditkartennummer ist einfach zu handhaben. Die Anmeldung an das System ist durch die Authentifizierung des Kunden und der Installation des Wallets mit Aufwand verbunden, der viele potentielle Anwender abschreckt. Auch die Verwaltung von Zertifikaten und der Transfer auf mobile beziehungsweise Zweitgeräte ist nicht einfach. Die Komplexität ist neben den Kosten der grösste Nachteil von SET.

#### Portabilität

Durch die persönlich zugeordneten Zertifikate, welche auf den Computer abgelegt werden, können die Bezahlungen nur auf dem Computer stattfinden auf dem das Zertifikat hinterlegt ist. Es ist möglich das Zertifikat auf ein anderes Gerät zu übertragen, dies ist jedoch mit einem grossen Aufwand verbunden. Die Portabilität ist somit nicht gegeben. Momentan wird versucht ein portables Wallet einzuführen. Dieses besteht aus einem Applet welches von einem im Internet verfügbaren Computer gestartet wird. Dies beeinträchtigt allerdings die Sicherheit des Systems.

#### Kosten

Die Kosten für den Kunden werden von den verschiedenen Anbietern individuell festgesetzt. Es wurde kein Anbieter gefunden, der eine Beteiligung an den Transaktionsbeträgen des Kunden verlangt. Die meisten Anbieter bieten Verträge mit einem Jahr Laufzeit zu einer festen Gebühr an.

#### Anonymität

Bei diesem Verfahren besteht eine teilweise Anonymität. Bei der Übermittlung der Daten bleiben die notwendigen Zahlungsdaten der Kreditkarte für den Händler verschlüsselt. Dieser erhält lediglich die Bestelldaten sowie gegebenenfalls die bei realen Gütern zur Warenlieferung benötigte Adresse. Die verschlüsselten Zahlungsdaten werden weiter zur Kreditkartengesellschaft geschickt. Dort wird kontrolliert, ob der Händler ein Vertragspartner ist. Des Weiteren wird das Kartenlimit überprüft und ob eine Sperre veranlasst wurde. Die Kreditkartenfirma hat keine Kenntnisse über die Lieferadresse oder die Bestellung des Kunden.

#### Image

Das Image von SET hat wegen der hohen Komplexität und der grossen Kosten, die oft auf den Kunden abgewälzt wurden, stark gelitten. Es gibt kaum noch Händler die SET anbieten.

#### Weitere Dienstleistungen

Neben der reinen Transaktionsabwicklung hat der Kunde natürlich die Möglichkeit die Vorteile einer Kreditkarte zu nutzen. Allerdings gibt es auch Anbieter die SET ohne eine reelle Kreditkarte, mit der man zum Beispiel eine Rechnung im Geschäft begleichen könnte, anbieten.

-Erfüllung der Anforderungen des Händlers

**Sicherheit vor Betrug**

Durch das Kundenzertifikat und die Zahlungsgarantie ist der Händler ausreichend vor Betrug geschützt.

**Kosten**

Die Kosten für den Händler sind im Vergleich zu anderen Bezahlssystemen relativ hoch. Da viele Anbieter eine fixe Gebühr pro Transaktion verlangen, ist das System für Micropayment nicht geeignet.

**Image**

Durch die hohe Komplexität des SET-Verfahrens für den Kunden konnte seit der Einführung von SET 1997 kein durchschlagender Erfolg verbucht werden. Es ist sehr schwer noch Payment Provider zu finden, die SET anbieten. Die Kreditkartengesellschaften scheinen von SET abzukommen und arbeiten an der Entwicklung neuer Standards. In den USA spielt SET „keine grosse Rolle“.

**Weitere Dienstleistungen**

Es werden keine weiteren Dienstleistungen angeboten. Das Mahn- und Rechnungswesen geht automatisch an den SET-Anbieter über.

## 4.2 Kreditkartenverfahren mit 3-D Secure

### 4.2.1 Komplexität

Visa und Mastercard haben die Integration dieses Verfahrens vollkommen an Drittanbieter ausgelagert. Diese kümmern sich meist um die Integration des MPI oder bieten entsprechende Schnittstellen für den Händler an. Der Händler behält die volle Kontrolle über die angebotenen Waren, da er die Produkt- und Preisverwaltung nicht aus der Hand gibt. Er erhält nur eine Bestätigung über den Erfolg der Transaktion. Der Aufwand für den Händler ist demnach gering. Für den Kunden ist der Vorgang sehr unkompliziert, vorausgesetzt er besitzt bereits eine Kreditkarte. Die Komplexität des Verfahrens ist für beide Parteien als gering einzuordnen.

### 4.2.2 Wirtschaftlichkeit

Der Händler muss einen Vertrag mit einem Paymentprovider abschliessen, welcher in Kosten und Abrechnungsmodell stark variiert. Die meisten Provider bieten 3-D Secure als Aufrüstooption für das normale Kreditkartenverfahren an und verlangen dafür, bei gleichem Disagio, eine einmalige Einrichtungsgebühr von ca. 250,00 €.

### 4.2.3 Erfüllung der Anforderungen

– Erfüllung der allgemeinen Anforderungen

**Atomicity**

Tritt ein Verbindungsabbruch bei Bestätigung der 3-D Secure Tauglichkeit des Kunden an den Händler ein Fehler auf, bricht dieser die Transaktion ab und es entsteht kein Schaden. Eine

mögliche Fehlerquelle ist ein Verbindungsabbruch nach dieser Bestätigung, der dazu führt, dass die eigentliche Kreditkartentransaktion nicht durchgeführt wird, obwohl der Händler die Bestätigung erhalten hat. Es ist nicht bekannt, wie die Anbieter dieses Problem lösen.

#### Consistency

Die Identifizierung des Kunden findet durch das Authorisierungsportal der kreditkartenvergebenden Bank statt. Der Händler sieht nur die Kreditkartendaten, die er an das Kreditkartenunternehmen weiterleitet.

#### Independency

Das Verfahren ist sowohl auf Seiten des Kunden als auch auf Seiten des Händler mit anderen Systemen kompatibel.

#### Durability

Da der Händler die Transaktionsbestätigung in Echtzeit erhält, ist das Risiko eines Datenverlustes relativ gering. Es wird davon ausgegangen, dass die eigentliche Kreditkartentransaktion von den beteiligten Anbietern ausreichend gesichert ist.

#### Internationalität

Das Verfahren profitiert von der Internationalität der Kreditkartenunternehmen.

#### Verlässlichkeit

Das Verfahren wird als sehr verlässlich eingestuft.

– Erfüllung der Anforderungen des Kunden

#### Sicherheit vor Datenmissbrauch

Durch die verteilte Verfügbarkeit von Kunden- und Identifikationsdaten, ist der Kunde vor Datenmissbrauch ausreichend geschützt.

#### Sicherheit vor Betrug

Das 3-D Secure Verfahren identifiziert den Händler.

#### Benutzerfreundlichkeit

Die Benutzerfreundlichkeit ist hoch. Die Anmeldung erfolgt online und dauert nur ein paar Minuten. Die einzelnen Transaktionen können allein durch Eingabe von Benutzerdaten abgeschlossen werden. Man sieht deutlich wie die Anbieter am Ausgleich der Nachteile von SET gearbeitet haben.

#### Kosten

Für den Kunden fallen keine weiteren Kosten zu seinen Kreditkartengebühren an.

#### Anonymität

Die Anonymität ist zum grösst möglichen Mass gegeben.

#### Image

Das Verfahren bekommt allgemein eine gute Kritik von Seiten der Händler und der Kunden. Durch die unkomplizierte Handhabung ist wohl mit einer Beteiligung der meisten

Kreditkartennutzer zu rechnen. Allerdings hat sich die Kreditkarte, zumindest in Deutschland, noch nicht als Zahlungsmittel etabliert.

#### Weitere Dienstleistungen

Es werden keine weiteren Dienstleistungen für den Kunden angeboten.

– Erfüllung der Anforderungen des Händler

#### Sicherheit vor Betrug

Die Anbieter geben eine Zahlungsgarantie und sichern sich durch die Unabstreitbarkeit der Transaktion durch den Kunden vor Chargebackforderungen ab, wälzen diese also auch nicht auf den Händler ab. Die Sicherheit vor Betrug ist demnach gross.

#### Kosten

Die Kosten sind abhängig vom Provider. Da es sowohl Anbieter mit Fixpreisen pro Transaktion als auch Anbieter mit prozentualer Beteiligung gibt, kann der Händler die Kosten an seine Bedürfnisse anpassen.

#### Image

Da die Nachteile von SET weitgehend abgeschafft wurden sollte, sich 3-D Secure recht schnell bei den Händlern etablieren. Weltweit gibt es bereits 11.000 registrierte Onlinehändler allein bei Visa, so zum Beispiel die Interkantonale Landeslotterie der Schweiz.

#### Weitere Dienstleistungen

Es gibt keine weiteren Dienstleistungen für den Händler.

## 4.2 Paybox / Moxmo

### 4.2.1 Komplexität

Entscheidet sich der Händler für die Integration von Moxmo / Paybox in seinen Shop hat, er zwei Möglichkeiten zur Verfügung. Entweder er leitet den Kunden nach Abschluss der Bestellung an eine Moxmo- / Payboxseite weiter, von der aus die Validierung des Kunden per Mobiltelefon abgewickelt wird, oder er integriert das entsprechende Protokoll selbst auf seiner Webseite. In beiden Fällen muss er nur einen Vorbildcode in seinen Shop integrieren. Beide Anbieter stellen bei einer Integration des Protokolls in den Shop, weitere Leistungen zur Validierung des Kunden zur Verfügung. Paybox hat ausserdem eine Reihe von Integrationspartnern, die sich um eine externe Bearbeitung der Transaktionen kümmern. In gewissen Abständen muss der Händler die Auszahlung der im Laufe der Zeit beim Anbieter angesammelten Zahlungen auf sein Konto beantragen. Der Kunde kann sich bei Paybox ohne eine postalische Validierung anmelden und das Angebot bis zu einem Limit sofort nutzen. Für die Anmeldung benötigt der Kunde das Mobiltelefon auf dessen SIM-Karte er in Zukunft zurückgreifen möchte. Zeitgleich mit der Anmeldung erhält der Kunde einen Vertrag den er unterschrieben an Paybox zurücksendet. Mit Erhalt des Vertrages wird das Limit aufgehoben. Moxmo verlangt vom Kunden eine PIN- Nummer zur Anmeldung, die dieser nach der Abbuchung der Jahresgebühr von seinem Konto erhält. Bis zur Eingabe der PIN- Nummer gibt Moxmo dem Kunden ein vorläufiges Limit von 25,00 €.

#### 4.2.2 Wirtschaftlichkeit

Moxmo verlangt eine Registrierung des Händlers, bevor Informationen zu den entstehenden Kosten gegeben werden. Allgemein wird von einer Jahresgebühr und einer „geringen Transaktionsbeteiligung“ gesprochen. Diverse Quellen aus dem Internet geben folgende Kosten an:

Jahresgebühr	250,00 € bis 2500,00 €
Transaktionsgebühren	3% bis 5% vom Bruttoumsatz
Gutschriftengebühr bei Auszahlung des Händlerkontos	3,00 €
Stornogebühren	0,25 €

Die Integration in den Shop ist, je nach gewählten Verfahren, einfach und verursacht keine grossen Kosten.

Paybox gibt die selben Preise für seine Leistungen an, verlangt aber zusätzlich eine Supportgebühr von 100,00 € bis 300,00 € pro Jahr, abhängig vom gewählten Integrationsmodell.

Die Kosten für den Kunden betragen 9,50 € pro Jahr bei Moxmo und 15,00 € pro Jahr bei Paybox. [Moxmo / Paybox]

In diesem Betrag sind alle Leistungen der Unternehmen gegenüber dem Kunden enthalten.

Die Firma ECS-Solution tritt als Integrationspartner von Paybox auf. ECS-Solution bietet dem Anbieter einen 24 Stunden Hilfsdienst über e-mail oder Helpdesk an. Sie übernimmt das ganze Inkassowesen sowie Stornierungen, welche für eine kleine Gebühr mitbearbeitet werden. Die Auszahlungen an die Händler findet alle 15 Tage statt.

Beispiel für Händlerkosten bei der Firma ECS-Solution: [ECS]

Einrichtungsgebühr	Keine
Monatliche Gebühr	Keine
Kosten pro Transaktion	0,29 Euro
Stornogebühren	7,50 Euro
Disagio	zwischen 7% und 13%

Vorteilig für den Händler ist die kostenlose Einrichtung sowie nur die Abrechnung pro Transaktion. Jedoch liegen die Stornogebühren sowie das Disagio ziemlich hoch. Ebenso wird das Disagio nach der Umsatzhöhe berechnet. Dieses System der Firma ECS-Solution ist nur für Unternehmen mit kleinem Jahresumsatz lohnenswert und zu empfehlen.

#### 4.2.3 Erfüllung der Anforderungen

-Erfüllung der allgemeinen Anforderungen

Atomicity

Da auch hier eine Abrechnung in Echtzeit stattfindet, ist die Atomicity gewährleistet.

### Consistency, Integrity

Alle beteiligten Parteien erhalten ihre Informationen, die sie zur Abwicklung benötigen. In diesem Falle benötigt nur Moxmo die personenbezogenen Daten sowie die Bankverbindung. Dritte Personen können lediglich während der Übertragung der Daten an Moxmo Zugriff auf diese erhalten. Dieses Risiko ist sehr gering, da die Daten mit SSL verschlüsselt werden.

### Independency

Auch für Paybox / Moxmo gilt, dass sowohl Händler als auch der Kunde noch weitere Bezahlssysteme anbieten beziehungsweise verwenden können.

### Durability

Da die Transaktionen direkt abgeschlossen werden geht das Verwahrungsrisiko zu dem entsprechenden Anbieter über. Es wird davon ausgegangen, dass sich dieser ausreichend gegen Datenverlust absichert.

### Internationalität

Weder Paybox noch Moxmo bieten ihr System ausserhalb Europas an. Moxmo beschränkt seine Dienstleistungen auf Kunden aus Deutschland und den Niederlanden. Paybox agiert in Österreich und Spanien.

### Verlässlichkeit

Das Verfahren ist von der telefonischen Erreichbarkeit des Kunden abhängig. Allerdings wird die Transaktion bei Nichterreichen des Kunden nicht durchgeführt. Es entsteht also kein Schaden, falls der Kunde nicht erreicht werden kann.

### -Erfüllung der Anforderungen des Kunden

#### Sicherheit vor Datenmissbrauch

Bei einem Missbrauch durch den Händler ist hier vorgesorgt. Die persönlichen Daten sind nur von Paybox / Moxmo bei der einmaligen Registrierung sichtbar. Der Kunde setzt seine Bestellung durch Eingabe seiner Mobiltelefonnummer durch. Der Händler erhält somit nur die Telefonnummer und bei Auslieferung von realen Gütern die Adresse.

#### Sicherheit vor Betrug

Da das Verfahren in gewissem Sinne eine Vorauszahlung darstellt, ist der Kunde vor einem Betrug des Händlers nicht geschützt.

#### Benutzerfreundlichkeit

Dem Kunden ist es bei internetfähigen Mobiltelefon möglich seine Bestellung ortsunabhängig zu tätigen. Der Aufwand bleibt gering, da der Käufer bei der Bestellung lediglich seine Mobiltelefonnummer angeben muss. Allerdings muss dieser auf Rückruf von Paybox / Moxmo warten, um die Zahlungstransaktion zu bestätigen. Die Anmeldung ist unkompliziert.

#### Portabilität

Da der Kunde sich über sein Mobiltelefon identifiziert, ist das System unabhängig vom verwendeten Computer oder internetfähigen Mobilgerät. Allerdings gibt der Kunde bei der Registrierung die Telefonnummer einer SIM-Karte an, von der er bei jeder Bestellung abhängig ist. Beim Wechsel des Mobiltelefons ist es einfach seine Registrierung auf eine neue Mobiltelefonnummer zu ändern. Moxmo bietet hierfür auf seiner Internetseite eine einfache

Reaktivierung auf ein neues Mobiltelefon an.

#### Kosten

Vom Kunden wird eine Jahresgebühr von 9.50 € (Moxmo) beziehungsweise 15,00 € (Paybox) verlangt. Dieser Preis ist erschwinglich und als positiv zu bewerten.

#### Anonymität

Dieses System hat eine teilweise Anonymität des Kunden. Der Händler erhält, vorausgesetzt es handelt sich um digitale Güter, keine persönlichen Informationen über den Käufer, ausser seiner Handynummer. Nur Moxmo verfügt über die persönlichen Angaben sowie dessen Bankverbindung.

#### Image

Durch die Insolvenz von Paybox.de hat das Image des Verfahrens zumindest in Deutschland stark gelitten. Auch wurden von den Konten der Payboxkunden nach der Insolvenz vereinzelt weitere Beträge abgebucht. Es ist abzuwarten wie sich das Image unter dem neuen Anbieter Moxmo entwickelt. Die vorläufige Resonanz scheint allerdings gut zu sein. In den anderen Ländern erfreut sich Paybox grosser Beliebtheit.

#### Weitere Dienstleistungen

Es ist möglich Geld von einem Paybox- / Moxmokonto auf ein anderes zu überweisen. Paybox bietet ausserdem Funktionen zum Bezahlen von Kino- und Theaterkarten sowie Parktickets per Handy an.

-Erfüllung der Anforderungen des Händlers

#### Sicherheit vor Betrug

Der Registrierungsprozess ist durch ein gestohlenen Mobiltelefon relativ leicht auszuhebeln, wodurch eine Belastung bis zum Limit des Anbieters möglich ist. Paybox bietet im Betrugsfall keine Zahlungsgarantie. Aus diesem Grund ist vor einer Verwendung im Macropaymentbereich abzuraten. Es gibt Unternehmen, wie zum Beispiel die Firma ECS-Solutions, die neben dem reinen Payboxsystem noch eine Adressvalidierung sowie eine Bonitätsprüfung anbieten.

#### Kosten

Die Kosten für den Händler sind im Vergleich zu anderen Bezahlssystemen sehr hoch. Der Händler muss sich entscheiden, ob ihm die gegebenen Vorteile, vorallem die Möglichkeit des Spontankaufs, die hohen Kosten wert sind.

#### Image

Auch die Händler wurden durch die Insolvenz von Paybox Deutschland abgeschreckt. Ausserhalb von Deutschland erfreut sich das Verfahren immernoch grosser Beliebtheit.

#### Weitere Dienstleistungen

Je nach Anbieter gibt es die Möglichkeit verschiedene Inkassovorgänge abzutreten.

## 4.3 Vorkasse

### 4.3.1 Komplexität

Die Integration ist sehr einfach, da keine sehr grossen Änderungen am Shop unternommen werden müssen. Extra angebundene Webseiten sind bei diesem Verfahren nicht notwendig. Es muss lediglich bei der Auswahl der Zahlungsart die Bezahlung per Vorkasse hinzugefügt werden. Der Händler erhält dann die Bestellung zusammen mit der Zahlungsart und muss nur noch auf die Überweisungsbestätigung des Kunden warten. Für eine Zuordnung von eingegangenen Überweisungen und noch ausstehenden Lieferungen ist ein gewisser Aufwand notwendig. Dieser Vorgang kann allerdings durch eine EDV-Lösung automatisiert werden.

### 4.3.2 Wirtschaftlichkeit

Die Kosten für den Vorgang werden vollständig auf den Kunden abgewälzt. Durch die Zuordnung der eingegangenen Zahlungen zu den entsprechenden Bestellungen entsteht ein zusätzlicher Aufwand, der allerdings als gering betrachtet werden kann. Die Kosten für den Kunden ergeben sich aus den Überweisungsgebühren der jeweiligen Bank und sind im Vergleich zu anderen Systemen zu vernachlässigen.

### 4.3.3 Erfüllung der Anforderungen

-Erfüllung der allgemeinen Anforderungen

#### Atomicity

Da die Transaktion nur aus der Sammlung der Bestellungen beim Händler und deren Abgleich gegen die Zahlungseingänge besteht, kann es keinen Abbruch des Vorgangs geben. Der Händler muss sich vor Datenverlust der gesammelten Lieferungen schützen.

#### Consistency, Integrity

Die Bank des Kunden erhält die Überweisungsdaten mit dem Zahlungszweck. Der Händler bekommt die Bestellung und gegebenenfalls die Adresse des Käufers. Die Konsistenz ist somit gegeben.

#### Independence

Die Unabhängigkeit zu anderen Systemen ist gegeben. Der Händler erhält lediglich die Bestellung, weitere Ausführungen auf dem Computer des Händlers sind nicht notwendig und behindern keine anderen Zahlungsverfahren in ihrer Abwicklung.

#### Durability

Die Überweisung wird im Bankencomputer gespeichert und kann im Notfall nachvollzogen werden. Des Weiteren besitzt der Kunde eine Überweisungsbestätigung. Die geschickte Bestellung wird vom Händler bestätigt, die wiederum der Kunde erhält. Die Dauerhaftigkeit ist gewährleistet. Der Kunde sollte bei der Bestellung eine Bestätigung erhalten, die er im Falle eines Datenverlustes beim Händler verwenden kann, um die Bestellung zu rekonstruieren.

#### Internationalität

Die Internationalität ist durch die jeweiligen Banken gegeben.

### Verlässlichkeit

Die Verlässlichkeit ist hoch.

-Erfüllung der Anforderungen des Kunden

### Sicherheit vor Datenmissbrauch

Bei der vorgenommenen Überweisung des Kundenkontos auf das Konto des Händlers, erhält der Händler lediglich die Information über den Namen des Überweisers sowie den Zahlungszweck und die Rechnungssumme. Da keine Angaben über die Bankverbindung, beispielsweise der Kontonummer, gemacht wird, ist es dem Anbieter oder anderen Personen nicht möglich weitere Überweisungen des Kundenkontos oder die Manipulation der Daten vorzunehmen. Es könnte lediglich ein Missbrauch der Adresse zustande kommen, während diese mit der Bestellung über das Internet an den Händler geschickt wird.

### Sicherheit vor Betrug

Der Kunde hat keine Möglichkeit sich vor einem Missbrauch durch den Händler zu schützen. Dies ist einer der Hauptgründe, warum der Kunde dem Verfahren kritisch gegenübersteht.

### Benutzerfreundlichkeit

Hier werden keine grossen Vorkenntnisse benötigt. Es wird lediglich die Bestellung sowie eventuell die Adresse zur Warenlieferung in einem Formular angegeben und durch Knopfdruck an den Händler verschickt. Die Überweisung der Rechnungssumme muss vom Kunden entweder über die Bank oder über online-banking veranlasst werden. Die Bedienung des Systems ist einfach, allerdings ist der Aufwand um die Überweisung zu tätigen zeitmindernd.

### Portabilität

Durch die Trennung von Bestellung und Überweisung kann die eigentliche Bestellung von jedem internetfähigen Gerät aus durchgeführt werden. Normale Überweisungen können bei allen Filialen der Kundenbank eingereicht werden.

### Kosten

Je nach Bank wird entweder pro Überweisung eine Gebühr verlangt oder eine pauschale Buchführungsgebühr. Meist werden für Onlineüberweisungen geringere Gebühren verlangt.

### Anonymität

Bei virtuellen Gütern erhält der Anbieter bei der Überweisung lediglich den Namen und den Überweisungszweck zu sehen. Hiemit ist fast eine vollständige Anonymität gegeben. Bei realen Gütern muss der Kunde neben der Bestellung auch seine Adresse angeben, womit die Anonymität aufgehoben ist.

### Image

Da keine dritte Instanz, ausser den Banken, denen im allgemeinen ein grosses Vertrauen entgegengebracht wird, beteiligt ist, ist das Image des Vorgangs vom Image des Händlers abhängig. Herkömmliche Verfahren zählen bei Kundenumfragen zu den meist erwähnten und somit zu den meist benutzten und bevorzugten Systemen. Der Verbreitungsgrad ist gross.

### Weitere Dienstleistungen

Es gibt keine weiteren Dienstleistungen

-Erfüllung der Anforderungen des Händlers

Sicherheit vor Betrug

Da der Händler das Geld vor dem Versand der Ware erhält, ist er vollkommen vor Betrug durch den Kunden geschützt.

Kosten

Dem Händler entstehen keine weiteren Kosten.

Image

Das Verfahren ist bei den Händlern wegen der 100%igen Zahlungssicherheit sehr beliebt.

Weitere Dienstleistungen

Es existieren keine weiteren Dienstleistungen.

## **5. Die Zukunft des E-Payment**

### 5.1 Gibt es ein bestes Verfahren?

Ein bestes Verfahren müsste sowohl Micro- als auch Makropaymentvorgänge für reelle und virtuelle Güter unterstützen. Allerdings gelten für die Wirtschaftlichkeit für jede dieser Kriterien verschiedene, teilweise gegensätzliche, Anforderungen. Bei den Micropaymentvorgängen geht es sowohl dem Kunden als auch den Händlern eher um geringe Kosten als um eine 100%ige Zahlungssicherheit. Bei virtuellen Gütern wird dieser Faktor noch verstärkt. Die Abrechnung reeller Güter im Macropaymentbereich benötigt allerdings eine hohe Zahlungssicherheit und eine eindeutige Validierung des Kunden. Dies ist mit grösserem Aufwand verbunden. Sollte ein Verfahren alle diese Kriterien abdecken wäre es für Micropaymentvorgänge nicht mehr rentabel. Es ist daher davon auszugehen, dass sich mehrere Systeme parallel entwickeln werden, die sich allerdings wegen der unterschiedlichen Zielgruppen nur wenig konkurrieren werden. Ausserdem ist davon auszugehen, dass sich pro Zielgruppe nur ein Verfahren bzw. Anbieter etablieren wird, da für jedes Verfahren eine Nutzerschwelle besteht, die überschritten werden muss, um auf dem Markt zu funktionieren. Hat ein Verfahren wenig Benutzer, wird es von wenigen Händlern angeboten und wird deswegen nur sehr schwer neue Kunden an sich binden können. Diese Nutzerschwelle macht es für neue Anbieter sehr schwer in das E-payment Geschäft einzusteigen.

### 5.2 Chancenlose Verfahren

Viele Verfahren, unter anderem E-Cash und Cybercoin wurden bereits eingestellt. Sicher ist allerdings, dass der Markt des E-Payment in den nächsten Jahren weiter wachsen wird und sich aus Gründen der Nutzerschwelle nur wenige Anbieter durchsetzen werden. Es ist davon auszugehen, dass sich einige unterschiedliche Verfahren für Macro- und Micropayment sowie für reelle und virtuelle Güter etablieren werden und für den jeweiligen Bereich eine Marktführungsposition einnehmen werden. Net900 und andere Anbieter, die auf einem Abbruch der laufenden Verbindung und einer Neueinwahl in ein teureres Netz aufgebaut sind, werden auf kurz oder lang vom Markt verschwinden. Erstens, wegen des schlechten Images durch „Dialer“- Viren, die diesen Vorgang unbemerkt vom Benutzer durchführen und zweitens, wegen der fehlenden Kompatibilität zu neuen Techniken wie W-Lan oder DSL. Ein Verfahren, das sehr mit dem hohen Installationsaufwand und

den grossen Anschaffungskosten zu kämpfen haben wird, ist die Geldkarte. Zwar bietet sie eine sichere und anonyme Zahlungsmethode, was sie auch für höhere Beträge qualifiziert, doch ist der Ladebetrag je nach Anbieter auf ca. 400 Euro beschränkt, was sie eher für Micropaymentvorgänge brauchbar macht. Dies steht allerdings zu den Anschaffungskosten im Widerspruch. Im normalen Geldverkehr wird die Geldkarte, auch wegen der grossen Unterstützung durch die Banken, weiterhin eine geläufige Alternative zum Bargeld darstellen. Die Rechnung im ursprünglichen Sinne wird wegen des hohen Risikos für den Händler eher seltener für E-Payment Vorgänge eingesetzt werden. Zwar ist sie für den Kunden einfach und unkompliziert, doch werden viele Händler auf gleichwertige, sicherere Verfahren umsteigen. Die Rechnung wird jetzt schon meist nur noch Stamm- oder Sonderkunden als Bezahlmethode angeboten. Verfahren die ohne persönlicher Validierung auskommen, wie Click & Buy, mögen zwar wegen des geringen Aufwands von Seiten des Kunden eine grössere Anzahl Nutzer ansprechen, doch ist eine Serie von Betrugsfällen zu erwarten, die das Vertrauen und damit die Marktposition stark schwächen werden. Wahrscheinlich werden diese Bezahlverfahren von Systemen mit Validierung verdrängt. In vielen Internetquellen wird das Kreditkartenverfahren über SET bereits als „Tot“ dargestellt. Hauptgrund hierfür ist die komplizierte Handhabung für den Kunden. Das Scheitern dieser Methode trotz grosser Unterstützung der einflussreichen Banken und Kreditkartengesellschaften zeigt deutlich, wie wichtig eine einfache Bedienbarkeit der Methode durch den Kunden ist. Prepaidkarten stellen zwar eine günstige Alternative zur Geldkarte dar, doch gibt es wegen der einfachen Realisierbarkeit eine zu grosse Anzahl von unterschiedlichen Anbietern. Um sich auf dem Markt zu etablieren, müsste sich entweder ein Anbieter hervorheben oder mehrere Anbieter müssten sich auf einen gemeinsamen Standart einigen, der es dem Händler ermöglicht durch die Wahl eines Anbieters alle anderen Prepaidkartensysteme zu bedienen.

### 5. 3 Zukunftsperspektiven

Dass sich in Zukunft neue Verfahren entwickeln werden, ist sicher. Da sich aber neue Verfahren erst durch einen grossen Kunden- und Anbieterstamm etablieren müssen, können nicht unbegrenzt neue Verfahren entwickelt werden. Die grosse Anzahl und kurze Lebensdauer von Verfahren schrecken den Kunden ab und erzeugen eine Abneigung gegen elektronische Bezahlverfahren. Um dies zu verhindern, muss eine Möglichkeit gefunden werden, dass sich einerseits der Kunde bei möglichst wenigen Stellen authentifiziert, andererseits dem Händler mehrere, in der Kostenstruktur auf seine Bedürfnisse angepassten Modelle zur Verfügung stehen. So kann zum Beispiel der Anbieter von Gütern im Micropayment keine Modelle verwenden die mit hohen Transaktionskosten verbunden sind. Da die Politik die Probleme des E-Business erkannt hat, wurden in den vergangenen Jahren die Forderungen nach einer rechtsgültigen digitalen Unterschrift laut. Diese könnte sowohl Zahlungssicherheit als auch eine Absicherung des Kunden garantieren. Auch die Anmeldeverfahren an bestehende Systeme würden weitaus unkomplizierter ausfallen. Der Händler wäre ausserdem nicht mehr an kostspielige Verfahren wie 3-D Secure gebunden, um den Kunden eindeutig identifizieren zu können. Allerdings tun sich alle Staaten mit der Umsetzung der digitalen Unterschrift schwer. Obwohl bereits 2001 ein Signaturgesetz in Deutschland eingeführt wurde, welches die elektronische Unterschrift der eigenhändigen gleichsetzt, gibt es bis jetzt kaum Anbieter die dies nutzen. Dies mag an der Beweislastumkehr liegen, durch die das Risiko im Fall einer Manipulation beim Signaturinhaber liegt, es sei denn er kann beweisen, dass es einem Anderen möglich war, die Signatur zu fälschen. Das Gesetz zur digitalen Unterschrift wurde in erster Hinsicht dafür entworfen dem Bürger den Gang zur Behörde zu ersparen. Banken und Kreditkartenunternehmen ist das Verfahren noch zu neu und unerprobt. Ausserdem wurde bis jetzt kein Standart für den Verschlüsselungsprozess definiert. Aus diesem Grund wurde 2003 von den

deutschen Parteien ein „Bündnis Für Elektronische Signaturen“ ins Leben gerufen, welche das Image der digitale Unterschrift verbessern sollte. Von einem Erfolg ist allerdings noch nichts zu spüren. Auch in der Schweiz lässt die digitale Unterschrift auf sich warten. Zwar wurden bereits 2003 erste Abstimmungen per Internet anhand einer digitalen Signatur durchgeführt, doch wurde der Zertifizierungsbetrieb bereits wieder eingestellt. Eine entgeltliche gesetzliche Regelung wird nicht vor 2005 erwartet. In Europa kann bis jetzt nur Finnland eine funktionierende digitale Unterschrift vorweisen. Seit 2000 kann dort die eigenhändige Unterschrift durch ein Zertifikat in Kombination mit einer staatlichen Identitätskarte ersetzt werden. Ob die digitale Unterschrift für den Internationalen Markt noch wirtschaftlich ist, wenn jedes Land ein eigenes Verfahren anbietet, bleibt abzuwarten. Einen anderen Weg wollen die Mitglieder der TCG gehen.

Die Trusted Computing Group (TCG) ist eine Allianz von Microsoft, Intel, IBM, HP und AMD die früher unter dem Namen TCPA auftrat. Diese Gruppe arbeitet an der Durchsetzung von TC, dem Trusted Computing. TC ist die Integration eines sicheren Chips in neue Computer, welcher durch mehrere Mechanismen vor den bis heute bekannten Manipulationsmöglichkeiten geschützt wird. Der TC-Chip, auch "Fritz-Chip" genannt, wird dabei beim starten des Rechners auf Unversehrtheit überprüft und schaltet das System dann in einen abgesicherten Modus, in welchem alle Daten, die den Prozessor passieren, zuerst dem Fritz-Chip zur Atorisierung vorgelegt werden. In erster Stufe können damit Manipulationen an Software verhindert werden, so zum Beispiel das Entfernen von Kopierschutzmechanismen. Die zweite Stufe baut auf eine im Chip integrierte Seriennummer auf, die es dem Anwender ermöglicht seine Dokumente nur für von ihm autorisierte Computer lesbar zu machen. Sollte sich TC durchsetzen, wird sich durch die eindeutige Identifizierung des Kunden das Bezahlwesen im Internet drastisch verändern. Der Kunde muss keine zeitraubenden Zertifizierungsprozeduren mehr über sich ergehen lassen. Ausserdem ist es möglich Dateien, die zum Beispiel E-Cash oder ähnliche Prepaidkonten repräsentieren, vor der Manipulation durch den Anwender zu schützen. Ebenso ist es dem Anbieter möglich, nicht den Download einer Ware zu berechnen, sondern deren tatsächliche Nutzung, also beispielsweise das Anhören eines Musikstückes. Die Übetragung von Waren von einem PC zu einem anderen kann untersagt werden und als Raubkopie identifizierte Daten global gesperrt werden.

Die Gegner von TC berufen sich auf die Tatsache, dass dieses Verfahren dem Benutzer grosse Restriktionen aufzwingt. Da alle auf einem PC erstellten Dokumente dessen Fritz-Chip-Seriennummer enthalten, ist es den verwaltenden Instanzen und damit auch den Regierungen möglich eine digitale Zensur vorzunehmen, in dem sie "Blacklists" in die Betriebssysteme der Kunden einbauen, die das Öffnen von bestimmten Dokumenten verbieten. Auch die OpenSource-Gemeinde steht dem Verfahren kritisch gegenüber, da es durch TC möglich ist Betriebssystemhersteller an Lizenzgebühren zu binden. Werden diese nicht bezahlt können mit dem Betriebssystem keine Daten eines teilnehmenden Betriebssystems geöffnet werden. Da mit AMD und Intel alle wichtigen CPU- Hersteller vertreten sind, ist es fraglich, ob sich nach einer Durchsetzung von TC ein "Parallelsystem" ohne diese Verfahren entwickeln wird. Sollte sich TC trotz der vielen kritischen Stimmen durchsetzen bleibt abzuwarten, ob es einen echten Mehrwert für elektronische Bezahlssysteme darstellt. So ist der Kunde fest an den PC gebunden, an dem er sich registriert hat. Einkäufe aus Internetcaffees, von mobilen Geräten oder von Computern von Bekannten werden nicht unterstützt. Man sieht, dass das Verfahren in ersten Linie entwickelt wurde, um die Softwarehersteller und Mediendistributoren vor Gewinneinbrüchen durch Raubkopien zu schützen und nicht zur Vereinfachung von Bezahlvorgängen im Internet.

## 6. Fazit

Es wurde gezeigt, dass keines der vorgestellten Verfahren für alle Bezahlvorgänge im Internet brauchbar ist. Viel mehr muss damit gerechnet werden, dass es für die verschiedenen Preisklassen und Arten der Güter verschiedene Verfahren geben wird, die parallel, eventuell sogar von einem grossen Anbieter, angeboten werden.

Im Macropaymentbereich möchte der Händler, wenn er reelle Güter anbietet, eine ausreichende Zahlungssicherheit. Hier kommen für ihn nur Vorkasse, Geldkarte oder Kreditkartenverfahren, bei denen eine Zahlungssicherheit garantiert wird, in Frage. Bei der Zahlung per Nachname muss der Händler die Transportkosten tragen, falls der Kunde die Annahme verweigert. Für den Kunden ist in dieser Preisklasse die Möglichkeit des Spontankaufs, also des Kaufs ohne grossen Registrierungsaufwand, meist nicht entscheidend. Er möchte sicher sein, dass er die bestellte Ware auch erhält. Er lehnt deswegen, in den meisten Fällen, die Prepaidverfahren ab. Für ihn ist, gerade bei grösseren Anschaffungen, die Zahlung per Nachname interessant, solange der Händler dieses anbietet. Da in diesem Bereich die Zahlung per Kreditkarte und 3-D Secure die meisten Bedürfnisse beider Seiten befriedigt, wird sich dieses Verfahren wahrscheinlich durchsetzen.

Bei virtuellen Gütern im Macropaymentbereich sind die Erwartungen der Parteien anders. Auch der Preis der angebotenen Güter ist meist deutlich geringer als bei realen Gütern. Virtuelle Güter befinden sich meist knapp oberhalb der Micropayment-grenze. In diese Kategorie fallen zum Beispiel Video- oder Musikdownloads sowie der Download von Software. Der Händler möchte hier ein möglichst grosses Publikum ansprechen, kann aber auch einen vereinzelt Zahlungsausfall verkraften, da für ihn dadurch kein echter Verlust entsteht. Er kann hier auf Paybox oder click & buy zurückgreifen, die es auch Kunden ohne Kreditkarte ermöglichen mehr oder weniger spontan einzukaufen. Der Verkauf von realen Gütern im Micropaymentbereich stellt, wegen der hohen Transportkosten, eher eine Ausnahme dar. Da Händler, wenn sie Micropaymentgüter anbieten, meist einen Mindestbestellwert verlangen, gelten hier die selben Bedingungen wie beim Macropayment. Virtuelle Güter im Micropaymentbereich sind meist Nachrichten- oder Informationsabos wie beispielsweise Wetterdaten oder das online Abrufen von Texten aus Magazinen und Zeitschriften. Auch hier hat die Zahlungssicherheit für den Händler keine grosse Relevanz. Er möchte es dem Kunden ermöglichen ohne viel Aufwand an die Güter zu gelangen, da dieser sonst versuchen wird auf anderem Wege an die Information zu kommen. Hier bietet sich click & buy an, da es dem Kunden keine weiteren Kosten verursacht und dieser sich innerhalb kürzester Zeit registrieren kann. Die Aussicht auf weitere Entwicklungen hat gezeigt, daß es auch in Zukunft viele verschiedene Ansätze geben wird um die Erwartungen der Teilnehmer am Zahlungsvorgang zu erfüllen. Eine staatliche, und damit rechtsgültige digitale Unterschrift wird den Authentifizierungsprozess vereinfachen. Allerdings stellt dies keine neue Bezahlmethode dar. Ob durch sie ein allgemeines Bezahlssystem, welches für alle Verwendungsmöglichkeiten akzeptabel ist, entstehen kann, bleibt fraglich. Trusted Computing geht, wenn man von den Sorgen der Gegner des Verfahrens absieht, in die richtige Richtung, muss aber mit einer Möglichkeit der mobilen Identifikation erweitert werden.

Als Hauptprobleme des E-Payments konnten die Nutzerschwelle, die ein Verfahren erreichen muss bevor es für Kunden und Händler interessant wird, die Komplexität des Verfahrens für den Kunden sowie der Schutz vor Zahlungsausfall gezeigt werden. Eventuell wird als Konsequenz ein staatliches Verfahren entwickelt, welches einerseits den Kunden an eine staatliche Zertifizierungstelle bindet, und andererseits die Banken zwingt den zertifizierten Händler Onlineauskünfte über die Kreditfähigkeit des Kunden zu geben. Dies wird allerdings schwer mit den Prinzipien der freien Marktwirtschaft und den gängigen Datenschutzrichtlinien zu vereinen sein.

## Literaturverzeichnis

- [E-Business 2003] Script Electronic Business, Prof. A. Meier, 2003
- [Heng 2004] Heng, Stefan: E-Payment: zeitgemässe Ergänzung traditioneller Zahlungssysteme; Deutsche Bank Research. available: [www.dbresearch.de/PROD/DBR\\_INTERNET\\_DE-PROD/PROD000000000078173.pdf](http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD000000000078173.pdf), zugegriffen am 25. April 2004
- [Henkel 2001] Henkel, Joachim: Anforderungen an Zahlungsverfahren im E-Commerce. In: R. Teichmann (Hrsg.): E-Commerce und E-Payment. Gabler Verlag, Wiesbaden 2001.
- [Kannen, Leischner 2001] Kannen, Martina; Leischner, Martin: E-Payment im Internet für kleine und mittlere Unternehmen. Hrsg.: Kompetenzzentrum Elektronischer Geschäftsverkehr Bonn / Rhein-Sieg. available: [www.inf.fh-bonn-rhein-sieg.de/person/professoren/leischner/e-payment.pdf](http://www.inf.fh-bonn-rhein-sieg.de/person/professoren/leischner/e-payment.pdf), zugegriffen am 20. April 2004
- [Arnold 2001] Arnold, Wolfgang: E-Payment-Systeme: Geld für den elektronischen Markt; Die Bank August 2001. available: [www.die-bank.de/media/082001/thema.pdf](http://www.die-bank.de/media/082001/thema.pdf), zugegriffen am 20. April 2004
- [Visa 2004] Visa: Visa Authenticated Payment Program, 3-D Secure. available: <http://international.visa.com/fb/paytech/secure/main.jsp>, zugegriffen am 10. Mai 2004
- [Anderson 2003] Anderson, Ross: Trusted Computing' Frequently Asked Questions; Version 1.1, August 2003. available: <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>, zugegriffen am 2. Mai 2004
- [IZV 2003] Information IZV: Informationen rund ums Thema „ Bezahlen im Internet“. available: [www.iww.uni-karlsruhe.de/izv/ergebnisse.html](http://www.iww.uni-karlsruhe.de/izv/ergebnisse.html), zugegriffen am 25. April 2004
- [Böhle, Riehm] Böhle, Knud; Riehm, Ulrich: Blümenträume – Über Zahlungssysteminnovationen und Internet-Handel in Deutschland. FIZ Karlsruhe 1998
- [Commerzbank 1998] Commerzbank: SET–Sicheres Bezahlen mit der Kreditkarte im Internet. available: <http://www.ecin.de/zahlungssysteme/set1/>, zugegriffen am 25. April 2004
- [Paybox] [www.paybox.at](http://www.paybox.at)
- [Moxmo] [www.moxmo.de](http://www.moxmo.de)

E-Payment

Eliane Fischer

[FIRSTGATE click&buy] [www.firstgate.de](http://www.firstgate.de)

[ECS] [www.ecs-solution.de](http://www.ecs-solution.de)