

E-Payment im Internet für kleine und mittlere Unternehmen



Kompetenzzentrum Elektronischer Geschäftsverkehr Bonn/Rhein-Sieg (KompEC)
gefördert vom Bundesministerium für Wirtschaft und Technologie (BMWi)

Impressum

Herausgeber: Kompetenzzentrum Elektronischer Geschäftsverkehr
KompEC Bonn/Rhein-Sieg
Bonner Talweg 17
53113 Bonn
Tel. (0228) 2284-133
Fax (0228) 2284-221
Internet: www.kompec.de
E-mail: kompec@bonn.ihk.de

Autoren: Dipl.-Inform. Martina Kannen
E-mail: martina.kannen@fh-bonn-rhein-sieg.de
Prof. Dr. Martin Leischner
Internet: www.martin-leischner.de
E-mail: martin.leischner@fh-bonn-rhein-sieg.de
Fachhochschule Bonn-Rhein-Sieg
Fachbereich Angewandte Informatik
Grantham-Allee 20
53757 Sankt Augustin
Internet: www.inf.fh-bonn-rhein-sieg.de

© Kompetenzzentrum Elektronischer Geschäftsverkehr KompEC Bonn/Rhein-Sieg, Juni
2001

Das Werk ist urheberrechtlich geschützt. Jede Verwendung außerhalb der Grenzen des
Urheberrechtsgesetzes ist ohne Zustimmung des KompEC Bonn/Rhein-Sieg unzulässig.

Inhaltsverzeichnis

1 Einleitung	5
2 Beschreibung von Internet-Zahlungssystemen	7
2.1 Lastschriftverfahren	7
2.2 Kreditkartensysteme	18
2.3 GeldKarte.....	36
2.4 paybox	44
2.5 net900 Classic	49
2.6 eCash	55
3 Auswahl und Einsatz von Internet-Zahlungssystemen	61
3.1 Strukturierter Planungsprozess	61
3.2 Auswahl der Internet-Zahlungssysteme	62
3.3 Outsourcing von Teilaufgaben an Payment-Service-Provider.....	67
3.4 Integration in das Online-Business - Checkliste	70
4 Liste Diensteanbieter für Internet-Zahlungssysteme	79
4.1 Anbieter von Internet-Zahlungssystemen	79
4.2 Payment-Service-Provider	84
Glossar	87
Literatur	97
Index	101

1 Einleitung

In den Anfängen des Internets spielten Eigentumsrechte und Warenaustausch gegen Geld keine Rolle. Das änderte sich zunächst auch nicht mit der Kommerzialisierung des Internets, als immer mehr Unternehmen begannen, sich mit einer eigenen Web-Site zu präsentieren. Ihr Ziel war es mit der Web-Präsenz ein positives Image aufzubauen. Hochwertige Inhalte (sogenannte Premium-Inhalte) wurden den Besuchern kostenfrei zur Verfügung gestellt. Finanziert wurde dies über Werbebanner.

Erst mit dem Aufkommen der Idee des Electronic Commerce, also dem Verkauf von Waren und Dienstleistungen über das Internet, wurde die Notwendigkeit von elektronischen Zahlungssystemen deutlich. Zum Einsatz gelangten zunächst vor allem die klassischen Bezahlverfahren, wie die Nachnahme und die Rechnung, die für den Händler einfach einzusetzen und den Kunden hinreichend bekannt sind. Diese pragmatischen Ansätze, die man auch heute noch in den meisten Internet-Shops vorfindet, werden den Anforderungen der Kunden und Händler im neuen Medium nicht gerecht.

Die Geschichte zeigt, dass sich das Bezahlen von Gütern immer wieder seiner Umgebung und Gesellschaft angepasst hat. Für das Zeitalter des Internets, einer zunehmend global agierenden und funktionsorientierten Gesellschaft, bedeutet dies die immer weitergehende Digitalisierung des Bezahlvorgangs und damit auch des Geldes. Geld wird zu einem technischen System, oder wie es so treffend auf der Homepage einer in Konkurs gegangenen Firma geschrieben stand: „Zahlen, die Geld bedeuten“.

Können wir also in naher Zukunft unser jetziges Geld in einem Museum betrachten, abgelöst durch Bits und Bytes? Zahlungssysteme, die dies ermöglichen würden, gibt es bereits. Doch die Hürden sind groß, damit sich ein solches System zur Bezahlung etabliert: So muss dieses neben (1) der allgemeinen Verfügbarkeit auch von (2) den Banken unterstützt werden; es muss (3) von Händlern als Bezahlmethode im Internet-Shop angeboten werden und letztendlich muss es (4) von Kunden als Zahlungsmittel akzeptiert werden. Und dies auch noch (5) in verschiedenen Ländern mit unterschiedlichen Kulturen, Mentalitäten und Rechtsprechungen. Diese gegenläufigen Interessen auszubalancieren kostet Zeit und Geduld. Hinzu kommt noch, dass es bei Zahlungssystemen schlicht und ergreifend um Geld geht, also um den Besitzstand von Menschen, Unternehmen und ganzer Volkswirtschaften.

Ein eindrucksvolles Beispiel für den mühsamen Prozess, ein Internet-Zahlungssystem auf dem Markt zu etablieren, liefert das System electronic cash. Der erste Pilotversuch hierzu startete bereits in den 70er Jahren, dem folgte 1981 der Beschluss der deutschen Kreditinstitute es einzuführen, worauf es dann 1990 realisiert wurde. Das System benötigte fast 20 Jahre um eingeführt zu werden!

Bislang gibt es kein Zahlungssystem für das Internet, das allen Bedürfnissen aller Beteiligten gerecht wird. Daher wird der Händler in der Regel gleichzeitig mehrere Zahlungssysteme in seinem Internet-Shop einsetzen, um keinen Kunden auf Grund des Bezahlverfahrens auszugrenzen. Doch die richtigen Zahlungssysteme hierzu auszuwählen, kann für den Händler ein schwieriges Unterfangen darstellen. Auf dem Markt gibt es eine Vielzahl von Internet-Zahlungssystemen; neue innovative Verfahren kommen laufend hinzu und klassische Systeme passen sich immer besser dem neuen Medium an, sie werden zunehmend „internettauglich“.

In dieser Situation soll Ihnen der vorliegende Leitfaden helfen, eine Übersicht über wichtige elektronische Zahlungssysteme im Internet zu gewinnen sowie die richtige Vorgehensweise für die Systemauswahl und die Integration in den Internet-Shop zu finden.

Zunächst werden in Kapitel 2 die Zahlungssysteme 'Lastschriftverfahren', 'Kreditkarte', 'Geldkarte', 'paybox', 'net900 Classic' und 'eCash' ausführlicher beschrieben. Sie erfahren wie das Bezahlen mit dem jeweiligen Zahlungssystem funktioniert, welche Kosten entstehen und welche Voraussetzungen Sie benötigen, um das Zahlungssystem im Internet einsetzen zu können. Das Kapitel 3 beschäftigt sich mit Auswahl und Einsatz von Internet-Zahlungssystemen. Es werden die einzelnen Schritte von der Definition der Anforderungen an das Zahlungssystem bis hin zur kundenorientierten Integration in den Internet-Shop dargestellt.

Im Anhang finden Sie eine Aufstellung von Dienstleistern und Anbietern von Zahlungssystemen mit Kontaktadressen sowie ein Glossar, das wichtige Begriffe im Umfeld von Zahlungssystemen erklärt.

2 Beschreibung von Internet-Zahlungssystemen

Wir beginnen mit zwei Zahlungssystemen, die sich bereits vor dem Internet als Bezahlverfahren etabliert haben, dem Lastschriftverfahren und der Kreditkarte und zeigen verschiedene Möglichkeiten der elektronischen Umsetzung im Internet auf.

Dem folgt die Beschreibung der Geldkarte als einem Beispiel für ein chipkarten-basiertes Zahlungssystem. Die Geldkarte wurde zur bargeldlosen Bezahlung in Parkhäusern, an Fahrkartenautomaten etc. entwickelt und kann seit einiger Zeit auch im Internet eingesetzt werden. Hierzu wird allerdings ein spezieller Chipkartenleser benötigt. Sollte dieser zu einer Standard-Komponente des PCs werden, dann hat die Geldkarte gute Chancen, sich als ein Zahlungssystem im Internet zu etablieren.

Im Weiteren werden drei Zahlungssysteme dargestellt, die speziell zur Bezahlung im Internet entwickelt worden sind: paybox als Beispiel eines Handy-basierten Zahlungssystems, bei welchem die Autorisierung der Zahlung über das Handy erfolgt. net900 Classic als Beispiel eines Inkassosystems, bei welchem die Beträge über einen bestimmten Zeitraum gesammelt und dann über die Telefonrechnung abgerechnet werden. Und abschließend eCash, welches zur Bezahlung digitale Münzen verwendet.

2.1 Lastschriftverfahren

Das Lastschriftverfahren ist ein klassisches Bezahlverfahren, das im Lastschriftabkommen gesetzlich geregelt ist und in dieser Weise nur in Deutschland existiert. Es ist bei den Kunden und den Händlern auf Grund seiner Einfachheit und seiner hohen Verbreitung gleichermaßen beliebt. Für den Händler ist das Lastschriftverfahren auch betriebswirtschaftlich sehr interessant, da er den Zahlungsvorgang auslöst (anders als bei der Überweisung) und die Gutschrift auf seinem Konto unmittelbar erfolgt.

Das EC-Lastschriftverfahren konnte sich als Bezahlssystem für Ladengeschäfte etablieren. Gegenwärtig werden damit 12% aller Bezahlvorgänge im Einzelhandel abgewickelt, mit der Kreditkarte lediglich 4%. Deshalb liegt es nahe, das Lastschriftverfahren auch im Internet anzubieten. Der Einsatz des Lastschriftverfahrens im Internet ist jedoch nicht einfach. Eine Hürde für die

Umsetzung stellt z.B. die erforderliche schriftliche Zustimmung des Kunden zum Kontoeinzug dar.

2.1.1 Wesen der Lastschrift

Das Lastschriftverfahren ermöglicht es dem Händler, Massenzahlungsverkehr einfach und rationell abzuwickeln. Mittels der Lastschrift, einem vom Kunden ausgefülltem Einzugspapier, lässt der Händler den jeweiligen Betrag vom Konto des Kunden abbuchen. Die Lastschrift enthält hierbei alle Angaben, die für den Einzug des Zahlungsbetrages vom Konto des Kunden notwendig sind:

Angaben im Lastschrift-Formular

- Name des Kunden,
- Kontonummer des Kunden,
- Bank des Kunden,
- Bankleitzahl der Kundenbank,
- Betrag,
- Verwendungszweck,
- Name des Händlers,
- Kontonummer des Händlers.

Lastschrift 216 501 10
000000

Sparkasse

Einzugsmächtigung des Zahlungspflichtigen liegt dem Zahlungsempfänger vor. Fristen und Termine für Fälligkeit, Vorlage und Rückgabe dürfen auf der Lastschrift nicht angegeben werden.

Zahlungspflichtiger: Name, Vorname/Firma (max. 27 Stellen)
Marianne Mustermann

Konto-Nr. des Zahlungspflichtigen **123456789** Bankleitzahl **12345678**

bei (Kreditinstitut)

* Bis zur Einführung des Euro (= EUR) nur DM; DM od. EUR; Betrag
DM **1000,00**

Verwendungszweck (Mitteln für den Zahlungspflichtigen) max. 2 Zeilen à 27 Stellen
Spende

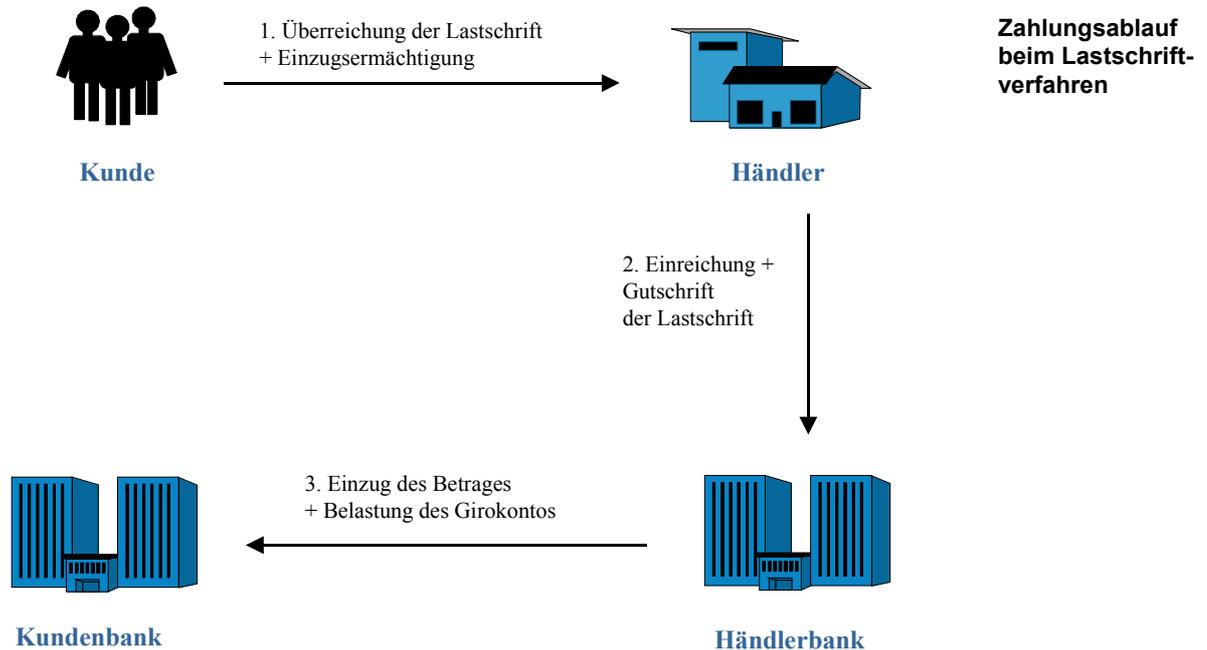
noch Verwendungszweck

Zahlungsempfänger: Name, Vorname/Firma (max. 27 Stellen)
Dt. Kinderkrebsstiftung

Konto-Nr. des Zahlungsempfängers **555666** 05

Beispiel einer Lastschrift

Der grundsätzliche Ablauf des Lastschriftverfahrens ist wie folgt:



Grundsätzlicher Zahlungsablauf beim Lastschriftverfahren

1. Überreichung der Lastschrift und Einzugsermächtigung

Der Kunde überreicht dem Händler die von ihm ausgefüllte Lastschrift sowie eine zugehörige, von ihm unterschriebene Einzugsermächtigung zum Konto-einzug.

2. Einreichung und Gutschrift der Lastschrift

Der Händler löst den Zahlungsvorgang aus, indem er die Lastschrift bei seiner Bank einreicht. Die Bank des Händlers prüft die Lastschrift auf Vollständigkeit und Plausibilität und schreibt den Zahlungsbetrag auf das Konto des Händlers gut (mit „Eingang vorbehalten“ E.v.).

3. Einzug des Betrages und Belastung des Girokontos

Die Bank des Händlers zieht den Zahlungsbetrag von der Bank des Kunden ein ohne das Kundenkonto auf ausreichende Deckung zur Einlösung der Lastschrift geprüft zu haben (Nachdisposition). Danach belastet die Bank des Kunden das Girokonto des Kunden um den Zahlungsbetrag.

Zustimmung des Kunden zum Einzug	<p>Voraussetzungen</p> <p>Dem Lastschriftverfahren geht voraus, dass der <i>Kunde</i> dem Einzug des Zahlungsbetrages von seinem Konto zustimmt. Dazu bieten sich dem Kunden zwei Möglichkeiten:</p> <ul style="list-style-type: none">• Der Kunde hinterlegt bei seiner Bank einen schriftlichen Abbuchungsauftrag, so dass die von einem bestimmten Händler vorgelegten Lastschriften eingelöst werden. Der Abbuchungsauftrag kann jederzeit widerrufen werden. Der Bank des Kunden liegt hier ein verbindlicher Auftrag vor, eine Rückgabe der Lastschrift wegen Widerspruch ist normalerweise nicht möglich. Der Abbuchungsauftrag wird hauptsächlich bei dauerhaften, festen Geschäftsbeziehungen zwischen Kunden und Händler eingesetzt.• Der Kunde erteilt dem Händler eine schriftliche Einzugsermächtigung, den jeweiligen Betrag von seinem Konto abzubuchen. Diese kann jederzeit widerrufen werden. Die Einzugsermächtigung liegt nicht der Bank des Kunden vor, sondern dem Händler. Die Erteilung kann mit der Lastschrift verbunden werden, indem der Kunde auf dem Lastschrift-Formular dem Einzug per Unterschrift zustimmt. Hat der Kunde dem Einzug des Zahlungsbetrages zugestimmt, kann er einer Lastschrift trotzdem innerhalb einer Frist von 6 Wochen¹ widersprechen, zum Beispiel weil ein falscher Betrag eingezogen wurde. Der Betrag wird ihm umgehend gutgeschrieben und beim Händler wiederum eingezogen.
Inkassovereinbarung zwischen Bank und Händler	<p>Der <i>Händler</i> muss zuvor mit seiner Bank eine sogenannte Inkassovereinbarung ("Vereinbarung über den Einzug von Forderungen durch Lastschriften") abschließen, damit er Lastschriften zum Einzug einreichen kann. Die Bank prüft hierzu die Bonität des Händlers und richtet gegebenenfalls eine Kreditlinie für den Lastschrifteinzug ein. In der Inkassovereinbarung verpflichtet sich der Händler, Lastschriften ordnungsgemäß einzureichen, da die Bank des Händlers für Schäden aus unberechtigt eingereichten Lastschriften haftet. Häufen sich beispielsweise Rücklastschriften wegen fehlender Einzugsermächtigung, dann kann die Inkassovereinbarung von der Bank gekündigt werden.</p>

¹ Aus wichtigen Gründen (z.B. Urlaub), kann der Kunde auch länger einer erfolgten Lastschrift widersprechen. Die 6-Wochen-Frist ist im Lastschriftabkommen festgeschrieben, dem der Zahlungspflichtige nicht beigetreten ist.

Kosten

Dem Kunden entstehen aus dem Lastschriftverfahren keine Kosten. Auch Lastschriftrückgaben beispielsweise wegen mangelnder Kontodeckung dürfen nicht mit Gebühren einhergehen.

Kosten für den Händler

Die Gebühren für den Händler pro Lastschrift werden von den Banken unterschiedlich abgegolten, z.B. über die Kontoführungsgebühr oder über eine Postengebühr. Kommt es zu einer Lastschriftrückgabe, dann fallen für den Händler 7,50 DM Gebühren seitens der Kundenbank zuzüglich der Kosten bei seiner Bank an.

Im *Ladengeschäft* des Händlers, auch als Point of Sale (POS) bezeichnet, haben sich neben der Kreditkartenzahlung zwei elektronische Zahlungssysteme etabliert, die beide in Kombination mit der EC-Karte funktionieren: das electronic cash System und das EC-Lastschriftverfahren.

Bezahlen im Ladengeschäft

Im Folgenden soll das electronic cash System, das *nicht* auf dem Lastschriftverfahren basiert, aus Gründen der Vollständigkeit kurz dargestellt werden.

electronic cash

electronic cash

electronic cash ist das von deutschen Banken favorisierte Zahlungssystem für das Ladengeschäft und wird vor allem bei Mineralölkonzernen² (Tankstellen) häufig eingesetzt. Der Händler muss einen Vertrag mit einem für electronic cash zugelassenen Netzbetreiber abschließen. Dieser stellt dem Händler electronic cash Terminals³ zur Verfügung und bindet diese an die jeweilige Bank an. electronic cash Terminals sind spezielle Lesegeräte für EC-Karten mit einer integrierten Tastatur zur Eingabe der PIN-Nummer. Möchte der Kunde über electronic cash bezahlen, dann verläuft das wie folgt:

- der Kunde schiebt seine EC-Karte in das Terminal,
- der Kunde gibt seine Geheimnummer (PIN) über die Tastatur des Terminals ein und bestätigt den zu zahlenden Betrag,
- das Terminal liest die Kontodaten aus der EC-Karte aus und sendet diese und die vom Kunden eingegebene PIN verschlüsselt an die Bank,
- die Bank prüft die PIN, die Bonität des Kunden und den Kontostand,
- die Zahlung wird dem Händler durch die Bank bestätigt oder abgebrochen.

Mit der Zahlungsbestätigung erteilt die Bank zugleich auch eine Zahlungsgarantie für den Zahlungsbetrag, womit das Risiko auf die Bank

² Dies lässt sich hauptsächlich aus der für Mineralölkonzerne günstigere Gebührenstruktur erklären.

³ Sogenannte EFT/POS-Terminals (Electronic Fund Transfer am Point of Sales) gemäß den Richtlinien des Zentralen Kreditausschusses (ZKA).

übergeht. Hierfür berechnet sie dem Händler Gebühren von 0,3% des getätigten Umsatzes, mindestens aber 0,15 DM. Für die Anbindung des Terminals an die Bank sowie für die Miete der Terminals entstehen dem Händler zusätzliche Kosten, die je nach Netzbetreiber variieren.

2.1.2 EC-Lastschriftverfahren

Da das electronic cash System für den Händler mit hohen Kosten verbunden ist, konnte sich das EC-Lastschriftverfahren, das auf eine PIN-Eingabe und eine Online-Anbindung zur Überprüfung der Daten durch die Bank verzichtet, schnell durchsetzen. Zur Zeit werden 12% aller Bezahlvorgänge im Einzelhandel mit dem EC-Lastschriftverfahren und nur 4% mit electronic cash abgewickelt.

Ablauf des EC-Lastschriftverfahrens

Das EC-Lastschriftverfahren funktioniert folgendermaßen:

- der Kunde schiebt seine EC-Karte in das Terminal,
- das Terminal liest die Kontodaten aus der EC-Karte aus und druckt diese automatisch auf einen Lastschriftbeleg,
- der Kunde unterschreibt diesen Lastschriftbeleg,
- der Händler überprüft die Unterschrift des Kunden mit der Unterschrift auf der Rückseite der EC-Karte,
- der Händler reicht die Lastschrift bei seiner Bank ein,
- die Bank prüft die Lastschrift und schreibt den Zahlungsbetrag auf das Konto des Händlers gut, die Bank des Händlers zieht den Zahlungsbetrag von der Bank des Kunden ein,
- die Bank des Kunden belastet das Konto des Kunden um den Zahlungsbetrag. Liegt keine Deckung für die Lastschrift vor, weist die Bank die Lastschrift zurück

Da bei diesem Verfahren lediglich durch den Vergleich der Unterschriften geprüft wird, ob es sich bei dem Kunden um den rechtmäßigen Besitzer der EC-Karte handelt⁴, besteht ein verhältnismäßig hohes Zahlungsrisiko, das ausschließlich der Händler trägt. Um ein eventuell notwendiges Inkasso für den Händler zu vereinfachen, gibt es auf dem Lastschriftbeleg einen Passus, in dem der Kunde unterschreibt, dass er im Falle einer Lastschrift Rückgabe mit der Weitergabe seines Namens und seiner Adresse einverstanden ist.

⁴ Bei einigen wenigen Ladengeschäften wie zum Beispiel bei der Bekleidungskette H&M muss zur Identifizierung noch zusätzlich der Personalausweis vorgelegt werden.

Häufig wird das EC-Lastschriftverfahren mit einer Prüfung von Sperrlisten kombiniert, um das Risiko des Zahlungsausfalls weiter zu minimieren. Sperrlisten sind Listen mit Zahlungskarten (EC-Karten, Kreditkarten), die beispielsweise wegen mehrerer Rücklastschriften nicht mehr akzeptiert werden. Die Terminals der Händler werden hierbei so miteinander verbunden, dass sie entweder auf eine überbetriebliche Handelssperreliste oder auf eine Händler-eigene Sperrliste zugreifen. Eine Zahlungsgarantie für den Händler gibt es nach wie vor nicht.

Für die Einreichung von Lastschriften fallen beim EC-Lastschriftverfahren keine weiteren Bankgebühren an.⁵

2.1.3 Lastschriftverfahren im Internet

Dem Händler bieten sich drei grundsätzliche Möglichkeiten an, das Lastschriftverfahren zur Bezahlung im Internet einzusetzen:

- die Bereitstellung des Lastschrift-Formulars,
- das Lastschriftverfahren mit SSL,
- das Lastschriftverfahren über einen Dienstleister.

Diese grundsätzlichen Möglichkeiten sollen folgend eingehender betrachtet werden.

A. Bereitstellung des Lastschrift-Formulars

Eine Möglichkeit für den Händler, das Lastschriftverfahren über das Internet anzubieten, besteht in der einfachen Bereitstellung des Lastschrift-Formulars über sein Internet-Angebot. Möchte der Kunde über das Lastschriftverfahren seine Zahlungen tätigen, füllt er online das Lastschrift-Formular aus, druckt es anschließend aus und unterschreibt auf dem Ausdruck die Zustimmung zur Einzugsermächtigung. Abschließend sendet er dem Händler das Formular per Postweg zu. Der Händler reicht die Lastschrift auf konventionellem Weg bei seiner Bank ein.

Diese Form des Lastschriftverfahrens über das Internet lässt sich technisch sehr einfach umsetzen. Jedoch schließt die Rücksendung der Lastschrift über den Postweg eine spontane Händler-Kunden-Beziehung aus.

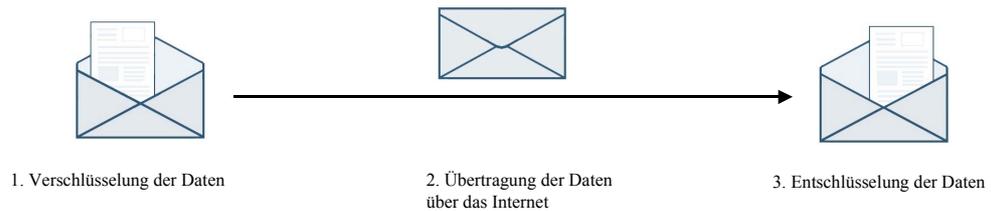
⁵ Die Banken hatten angekündigt, künftig für jede eingereichte Lastschrift aus dem EC-Lastschriftverfahren eine Bearbeitungsgebühr von 0,45 DM zu erheben. Dieser Ankündigung ist am 07.03.2001 vom Bundeskartellamt [BUN] widersprochen worden.

B. Lastschriftverfahren mit SSL

Um den Medienbruch über den Postweg zu vermeiden, besteht eine weitergehende Variante des Lastschriftverfahrens darin, dass der Kunde das ausgefüllte Lastschrift-Formular direkt über das Internet an den Händler sendet. In diesem Fall muss sich der Händler mit Sicherheitsmaßnahmen zum Schutz der Kundendaten auseinandersetzen, weshalb im Folgenden kurz auf das SSL (Secure Socket Layer)-Protokoll eingegangen wird.

Verschlüsselung mit SSL

SSL hat die Aufgabe die vertraulichen Daten des Kunden, wie zum Beispiel die Kontonummer, verschlüsselt bis zum Internet-Rechner des Händlers zu übertragen, so dass kein Dritter unbemerkt die Angaben lesen oder verändern kann. Die Verschlüsselung schützt das vom Kunden ausgefüllte Formular, ähnlich wie ein zugelebter Briefumschlag den Inhalt eines Briefes schützt.



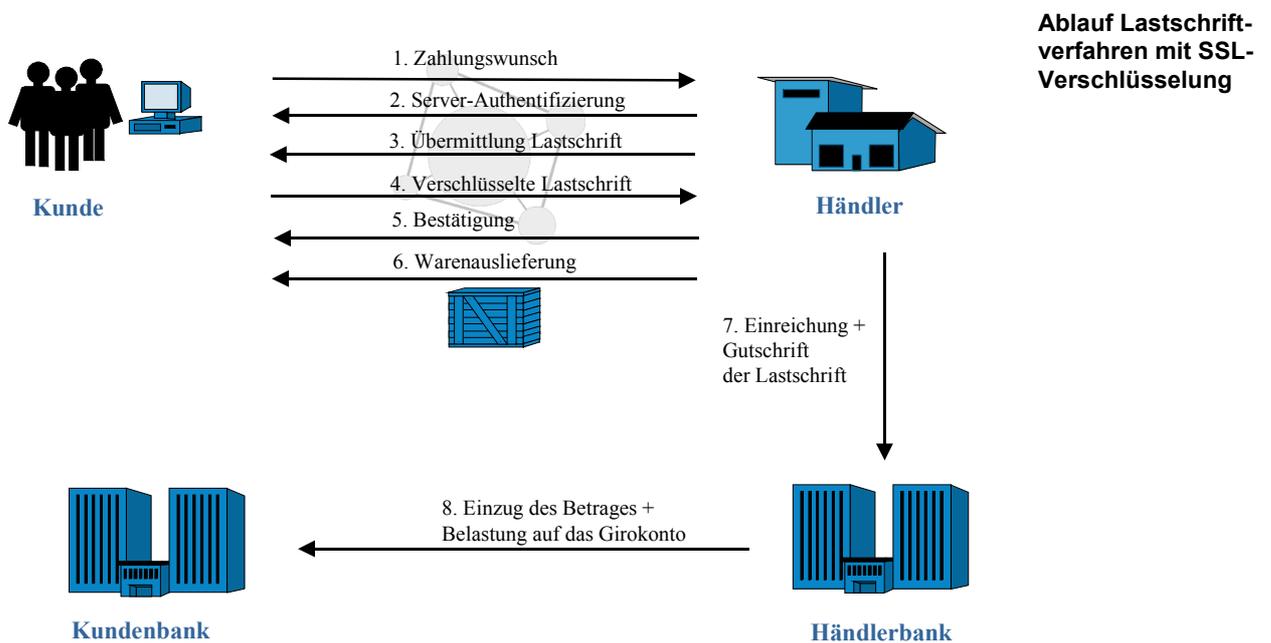
Prinzip der Verschlüsselung

SSL ermöglicht zusätzlich eine sogenannte Server-Authentifizierung, d.h. der Kunde erhält eine Bestätigung darüber, dass es sich beim Kommunikationspartner um den Rechner des Händlers handelt, an welchen die Lastschrift versendet wird. Diese Bestätigung, das Zertifikat, ist vergleichbar mit einem Personalausweis, der zum Beweis der Identität vorgelegt wird. Damit soll vermieden werden, dass der Kunde die Lastschrift an einen Rechner sendet, der fälschlicherweise vorgibt, der Rechner des Händlers zu sein (sogenannte 'man in the middle'-Attacke).



Beispiel eines Zertifikats

Das Lastschriftverfahren mit SSL-Verschlüsselung verläuft wie folgt:



Ablauf Lastschriftverfahren mit SSL-Verschlüsselung

Zahlungsablauf Lastschriftverfahren mit SSL

1. Zahlungswunsch

Der Kunde wählt im Online-Angebot des Händlers das Lastschriftverfahren mit SSL aus, um seine Zahlung zu tätigen.

2. Server-Authentifizierung

Der Kunde bekommt eine Bestätigung (Zertifikat) angezeigt, dass es sich um den Rechner des Händlers handelt.

3. Übermittlung der Lastschrift

Dem Kunden wird das Lastschrift-Formular übermittelt.

4. Verschlüsselte Lastschrift

Der Kunde füllt das Online-Formular aus und sobald er mit der Maus auf den Absende-Button klickt, wird das Formular verschlüsselt über das Internet an den Händler gesendet. Der Kunde bekommt die Bestätigung der Verschlüsselung seiner Daten in seinem Internet-Browser entsprechend angezeigt, beim Netscape Navigator beispielsweise durch das Schließen eines Schlosses. Erst auf dem Internet-Rechner des Händlers wird das Formular entschlüsselt.

5. Bestätigung

Der Kunde erhält eine Bestätigung, dass der Händler die von ihm ausgefüllte Lastschrift empfangen hat.

6. Warenlieferung

Der Händler kann nun die Warenauslieferung in die Wege leiten.

7. Einreichung und Gutschrift der Lastschrift

Der Händler reicht die Lastschrift, ohne Einzugsermächtigung des Kunden, bei seiner Bank ein. Die Bank des Händlers prüft die Lastschrift auf Vollständigkeit und Plausibilität und schreibt den Zahlungsbetrag auf das Konto des Händlers gut (mit „Eingang vorbehalten“ E.v.).

8. Einzug des Betrages und Belastung des Girokontos

Die Bank des Händlers zieht den Zahlungsbetrag von der Bank des Kunden ein. Die Bank des Kunden belastet das Konto des Kunden um den Zahlungsbetrag. Erst nach der Buchung wird das Kundenkonto auf ausreichende Deckung zur Einlösung der Lastschrift geprüft (Nachdisposition).

**SSL-fähiger
Browser**

Für das Lastschriftverfahren mit SSL ist es notwendig, dass der Kunde einen SSL-fähigen Internet-Browser nutzt. Das ist heute in der Regel der Fall; nur sehr alte Browser unterstützen das SSL-Protokoll nicht. Der Internet-Server des Händlers, auf welchem das Online-Lastschrift-Formular abgelegt ist, muss

ebenfalls SSL unterstützen. Für die Server-Authentifizierung benötigt der Händler zusätzlich ein Zertifikat, das seine Identität bestätigt. Zertifikate werden von sogenannten vertrauenswürdigen Instanzen, auch Zertifizierungsstellen oder Trust Center genannt, gegen eine Gebühr ausgestellt.

Das Lastschriftverfahren in der hier aufgezeigten Form im Internet anzubieten, ist mit vielen Unsicherheiten für den Händler verbunden. Das größte Problem besteht darin, dass der Kunde der Einzugsermächtigung online nicht zustimmen kann, da hierzu seine Unterschrift erforderlich ist⁶. Auch der Passus bei manchen Online-Lastschrift-Formularen, dass mit dem Ausfüllen und Absenden der Lastschrift dem Einzug zugestimmt wird, ist rechtlich nicht ausreichend. Die rechtliche Situation hierzu verdeutlicht das Beispiel eines Bankers: Wenn man einen Wecker über das Lastschriftverfahren kauft, ohne dem Kontoeinzug zuzustimmen und sich 7 Monate von dem Wecker wecken lässt, dieser eines Morgens jedoch nicht mehr funktioniert, dann kann der Wecker zurückgegeben und die Lastschrift rückgängig gemacht werden, da die Einzugsermächtigung fehlt.

Ein weiteres Problem ist die fehlende Überprüfung der Kundenbonität und der Richtigkeit der Kontodaten. Diese müssen vom Kunden manuell in das Online-Formular eingetragen werden und können bislang nicht wie beim EC-Lastschriftverfahren automatisch über ein Terminal ausgelesen werden. Die Gefahr besteht, dass der Kunde versehentlich oder absichtlich die Daten falsch eingibt. (Die meisten Lastschriften werden jedoch wegen mangelnder Kontodeckung abgewiesen.) Mit Rücklastschriften sind nicht nur Bankgebühren von mindestens 7,50 DM verbunden, sondern häufig auch die Rückforderung bereits ausgelieferter Ware.

C. Lastschriftverfahren über einen Dienstleister

Um das Risiko der Lastschrift Rückgabe zu reduzieren, gibt es eine Vielzahl von Dienstleistern, die verschiedene Services rund um das Lastschriftverfahren anbieten. Einige Beispiele hierzu:

- Die Kontodaten des Kunden werden auf Plausibilität geprüft, beispielsweise ob die angegebene Bankleitzahl existiert und ob die Kontonummer die notwendige Anzahl von Ziffern aufweist.

⁶ Im neuen Signaturgesetz ("Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften") [INT], das die EG-Richtlinien umsetzt und am 15.02.2001 vom Bundestag beschlossen wurde, sind sogenannte qualifizierte Signaturen vorgesehen, die die Schriftform ersetzen sollen. Künftig könnten mit einer solchen Signatur die Erteilung von Einzugsermächtigungen auch online erfolgen.

- Es wird überprüft, ob für den Kunden ein Eintrag in einer händlerübergreifenden Sperrdatei vorliegt.
- Die Zahlungsdaten werden über eine Online-Anbindung der Bank zur Überprüfung der Kontodeckung weitergeleitet.
- Die Kundendaten wie z.B. Wohnort oder E-Mail-Adresse werden einer Bewertung⁷ hinsichtlich der Bonität unterzogen.
- Bei Zahlungsverweigerung des Kunden werden Mahnungen verschickt und - falls notwendig - das Inkassoverfahren eingeleitet und betrieben.
- Der Kunde muss sich vor der Bezahlung beim Dienstleister registrieren, um eine Zugangsberechtigung zu bekommen. Er erhält eine persönliche Zugangskennung wie zum Beispiel ein Passwort, mit welchem er sich beim Bezahlen per Lastschriftverfahren identifiziert. Die Zugangskennung wird dabei mit den zugehörigen Kundendaten überprüft.

2.2 Kreditkartensysteme

Die Kreditkarte wurde Ende der 50er Jahre ursprünglich für vielreisende und wohlhabende Geschäftsleute sowie Privatiers eingeführt, um diese der Notwendigkeit zu entheben, bei ihren Reisen und Freizeitgestaltungen größere Summen in der jeweiligen Landeswährung mitführen zu müssen⁸.

Heute ist die Kreditkarte ein weltweit akzeptiertes Zahlungsmittel, das internationale Zahlungen ohne Probleme ermöglicht. In den USA wird die Kreditkarte häufiger zum Bezahlen genutzt als das Bargeld. In Deutschland verfügen rund 10 Millionen Kunden über eine Kreditkarte, wobei die Hälfte auf den Marktführer Eurocard entfallen.

Auf jeder Kreditkarte sind die Kreditkartennummer, der Name des Kreditkarteninhabers und das Verfallsdatum in hochgeprägten Zeichen aufgedruckt. Die Hochprägung ermöglicht es, Papierbelege des Zahlungsvorgangs zu erstellen.

⁷ Dies geschieht mit sogenannten Scoring-Modellen, welche mit Hilfe statistischer Methode den Kunden einen Score zuteilen. Kunden mit gutem Score wird die Zahlung per Lastschrift gewährt.

⁸ Kreditkarten für ausschließlich diesen Zweck werden als Travel & Entertainment- (T&E-) Card bezeichnet. Aus diesem Grund sind bei Kreditkarten in aller Regel Versicherungen (z.B. Auslandsranken- oder Gepäckversicherungen) mit inbegriffen.



Beispiel einer Kreditkarte

Die Kreditkarte zählt zu den klassischen Zahlungssystemen, die sich neben dem Bargeld und der EC-Lastschrift sowie dem electronic cash im Ladengeschäft etablieren konnten. Der Händler muss hierzu Akzeptanzstelle für die jeweilige Kreditkarte sein: so kann ein Kunde mit seiner Visa-Karte nicht bei einem Händler bezahlen, der ausschließlich die Eurocard akzeptiert. Daher wird der Händler in der Regel mehrere Karten akzeptieren.

Bei der Kreditkartenzahlung gibt es folgende Teilnehmer:

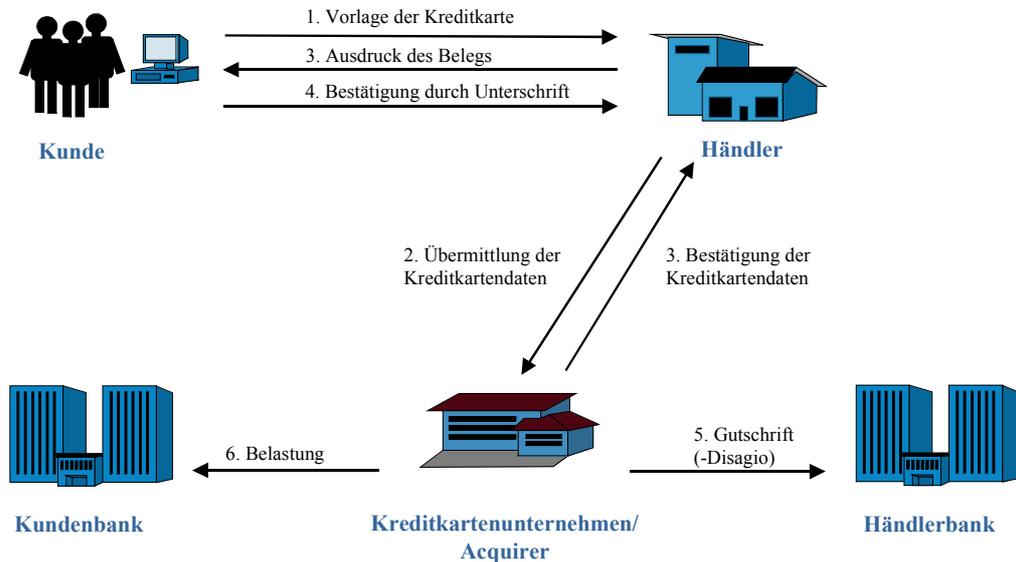
Teilnehmer

- der Kunde, der als Karteninhaber mit der Kreditkarte zahlt,
- der Händler, der die Zahlung per Kreditkarte anbietet bzw. akzeptiert. Er tritt als Akzeptanzstelle für Kreditkarten auf und wird von Seiten der Kreditkartengesellschaften als Vertragspartner bezeichnet,
- die Kreditkartengesellschaften, wie zum Beispiel Visa, Euro/ Mastercard oder American Express,
- die Kundenbanken, auch Issuer genannt, welche die jeweiligen Kreditkarten im Auftrag der Kreditkartengesellschaft an die Endkunden herausgeben,
- die Händlerbanken, auch Acquirer genannt, die für die Kreditkartengesellschaften die Abwicklung von Verträgen und Transaktionen sowie für die Betreuung der Vertragspartner zuständig sind. D.h. die Kreditkartengesellschaften unterhalten in der Regel keine direkte Kundenbeziehungen, sondern werden durch die Händlerbanken vertreten.

Eine Kreditkartenzahlung im Ladengeschäft verläuft wie folgt⁹:

⁹ Der Ablauf der Kreditkartenzahlung unterscheidet sich je nach Kreditkartentyp und hängt davon ab, ob ein Acquirer zwischengeschaltet ist oder nicht. Zudem muss das Lesegerät

**Ablauf einer
herkömmlichen
Kreditkarten-
zahlung**



Ablauf einer herkömmlichen Kreditkartenzahlung

1. Vorlage der Kreditkarte

Der Kunde legt dem Händler zur Bezahlung der Ware oder Dienstleistung seine Kreditkarte vor.

2. Übermittlung der Kreditkartendaten

Der Händler zieht die Kreditkarte des Kunden durch ein spezielles Lesegerät, welches mit der Kreditkartengesellschaft oder einem Acquirer online verbunden ist. Das Lesegerät liest die Kreditkartennummer, den Namen des Kreditkarteninhabers und das Verfallsdatum der Kreditkarte vom Magnetstreifen aus und sendet diese Daten sowie die Daten des Händlers (Betrag, Händler-Nummer) an die Kreditkartengesellschaft/Acquirer zur Genehmigung.

3. Bestätigung der Kreditkartendaten

Die Kreditkartengesellschaft/Acquirer überprüft an Hand der Daten, ob die Kreditkarte gültig ist, kein Eintrag in einer Sperrliste vorliegt und ob der eingeräumte Verfügungsrahmen eingehalten wird. Bei Genehmigung sendet die Kreditkartengesellschaft/Acquirer dem Händler eine Bestätigung über die erfolgte Zahlung sowie eine Autorisierungsnummer, die für eine Zahlungsga-

zur Akzeptanz von Kreditkartenzahlungen nicht mit der Kreditkartengesellschaft/Acquirer online verbunden sein. Offline-Zahlungen werden von den Kreditkartengesellschaften jedoch nur bis zu einem bestimmten Betrag genehmigt und sind zudem mit einem höheren Disagio verbunden.

rantie steht. Gleichzeitig wird die Transaktion bei der Kreditkartengesellschaft intern verbucht.

4. Ausdruck des Belegs

Das Lesegerät beim Händler druckt den zur Zahlung gehörenden Beleg aus und der Händler legt diesen dem Kunden zur Unterschrift vor.

5. Bestätigung durch Unterschrift

Der Kunde bestätigt die Zahlung, in dem er den Beleg unterschreibt. Der Händler überprüft diese mit der Unterschrift auf der Rückseite der Kreditkarte.

6. Gutschrift auf das Girokonto

Die Kreditkartengesellschaft/Acquirer überweist den Zahlungsbetrag auf das Girokonto des Händlers, abzüglich eines Disagios.

7. Belastung des Girokontos

Im Gegenzug belastet die Kreditkartengesellschaft/Acquirer das Konto des Kunden mit dem Zahlungsbetrag, normalerweise zu einem späteren Zeitpunkt (abhängig vom Vertrag).

Voraussetzungen

Kreditkarten können über die Banken sowie über eine Vielzahl anderer Dienstleister, wie z.B. den ADAC, erworben werden. Voraussetzung hierfür ist:

- die Volljährigkeit des Antragstellers,
- eine hinreichende Bonität, die beispielsweise über eine Schufa-Auskunft geprüft wird,
- die Angabe eines Girokontos, über welches das Kartenkonto abgewickelt wird.

**Voraussetzungen
für den Kunden**

Mit dem Erwerb der Karte ist der Kunde berechtigt bei jedem Händler, der die entsprechende Kreditkarte akzeptiert, Leistungen ohne Bargeldzahlung gegen Vorlage der Kreditkarte in Anspruch zu nehmen. Der Kunde erhält eine monatliche Übersicht über alle von ihm getätigten Zahlungen, der Gesamtbetrag wird ihm vom Konto abgebucht. Der Karteninhaber ist verpflichtet, auf seinem Bankkonto für eine hinreichende Deckung zu sorgen. Eventuelle Überziehungen gehen zu Lasten des Bankkontos und nicht des Kreditkar-

tenkontos. Daher handelt es sich bei diesen - in Deutschland üblichen - Karten nicht um „echte“ Kreditkarten, sondern lediglich um Charge-Karten.

Voraussetzungen für den Händler

Der Händler muss, um Kreditkartenzahlungen anzubieten, zunächst eine offizielle Akzeptanzstelle für Kreditkarten werden. Dazu muss er mit der jeweiligen Kreditkartengesellschaft oder mit einem entsprechenden Acquirer, einen Händlervertrag abschließen. Die Vertragsschließung über einen Acquirer bietet sich vor allem an, wenn dieser für mehrere Kreditkarten Akzeptanzen vergibt. In dem Vertrag werden die Gebühren und weitere Zahlungsbedingungen geregelt. Der Händler erklärt sich in dem Vertrag bereit, die Kreditkarte als Zahlungsmittel zu akzeptieren¹⁰. Die Kreditkartengesellschaft sichert dem Händler in vertraglich festgelegten Grenzen Zahlungsgarantien zu, wenn dieser vorgegebene Kontrollmaßnahmen bei der Bezahlung vornimmt (etwa die Überprüfung der geleisteten Unterschrift). Nach Abschluss des Vertrages erhält der Händler eine Vertragsunternehmensnummer (VU-Nummer), mit welcher er sich gegenüber der jeweiligen Kreditkartengesellschaft/Acquirer identifiziert. Sollen mehrere Währungen akzeptiert werden, muss die VU-Nummer multiwährungsfähig sein.

Kosten

Kosten für den Kunden

Je nach kartenausgebender Bank muss der Kunde für seine Kreditkarte eine jährliche Gebühr zwischen 10,- und 30,- DM bezahlen. Ansonsten verursacht die Kreditkarte bzw. die Zahlung mit dieser keine weiteren Kosten für den Kunden.

Kosten für den Händler

Bei der Akzeptanz von Kreditkartenzahlungen entstehen dem Händler folgende Kosten:

- 2-4% Disagio vom Bruttoumsatz pro Kreditkartenzahlung. Die Höhe des Disagios ist u.a. abhängig vom Vorjahresumsatz und vom Zeitpunkt der Wertstellung. Eine schnellere Wertstellung der Kreditkartenumsätze ist auch mit einem höheren Disagio verbunden.
- Eine Überprüfungsgebühr zwischen 0,13 und 1,35 DM pro Transaktion, die online autorisiert wird.
- Kosten für das Karten-Lesegerät sowie im Falle einer Online-Anbindung zusätzliche Kommunikationskosten.

¹⁰ Hierbei handelt es sich um einen Vertrag zu Gunsten Dritter (Karteninhaber).

2.2.1 Kreditkartenzahlungen mit SSL

Kreditkartenbasierte Zahlungssysteme sind sehr einfach im Internet einsetzbar, denn anders als beim Lastschriftverfahren ist die Kreditkartenzahlung von den gesetzlichen Rahmenbedingungen her nicht an eine Unterschrift gebunden.

Um Kreditkartenzahlungen im Internet akzeptieren zu können, muss der Händler mit der Kreditkartengesellschaft einen speziellen Vertrag abschließen, den sogenannten MOTO-Vertrag (Mail-Order/ Telephone-Order). Mit dem MOTO-Vertrag erklärt sich der Händler einverstanden, dass der Kunde die Zahlungen nicht mit seiner Unterschrift bestätigen muss. Widerspricht der Kunde einer Zahlungsabbuchung, bekommt er den Betrag umgehend von der Bank gutschrieben. Der Händler trägt hierbei das Risiko, denn die Kreditkartengesellschaft leistet bei MOTO-Verträgen keine Zahlungsgarantien.

Um das Risiko für den Händler zu reduzieren, dass ein Kunde widerrechtlich fremde Kreditkartendaten eingibt, die zwar gültig, jedoch nicht ihm zugehörig sind¹¹, müssen Eurocard- und Visa-Kunden bei Zahlungen im Internet ab dem 1. April 2000 zusätzlich eine dreistellige Kartenprüfnummer (Card Verification Code 2, CVC2) angeben. Diese kann bei einer Online-Anbindung an eine Autorierungsstelle zusätzlich abgefragt und überprüft werden. Die Kartenprüfnummer befindet sich auf der Rückseite der Kreditkarte hinter der zwölfstelligen Kreditkartennummer im Unterschriftsfeld.¹²



Rückseite einer Kreditkarte

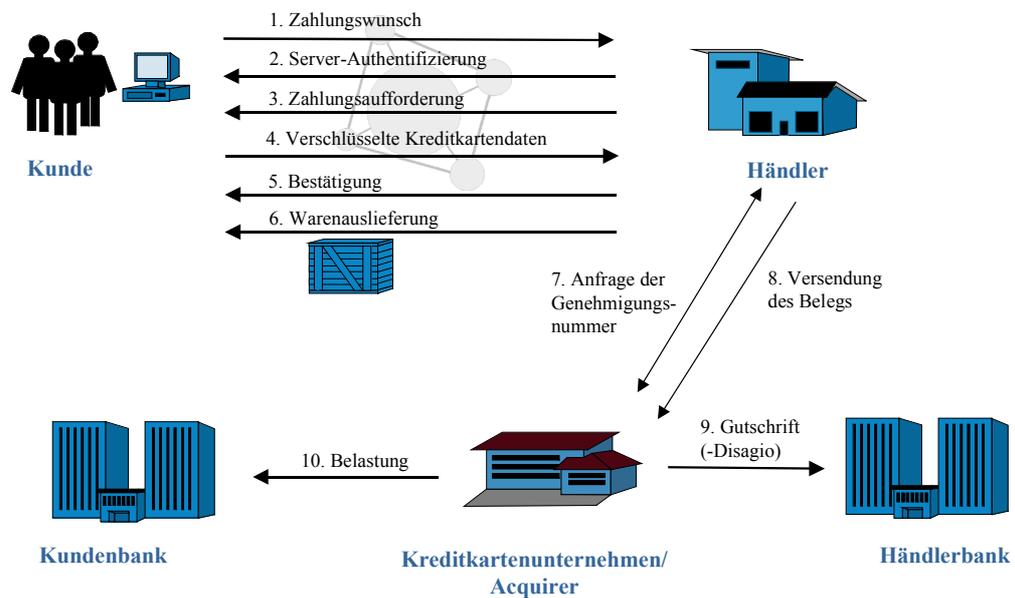
¹¹ Nach Aussagen von Eurocard stieg im Jahr 2000 das Betrugsvolumen bei Kreditkartenzahlungen im Internet um rund 32 Prozent an. Der Schaden beträgt rund zwölf Millionen Mark pro Jahr (= ca. 5 Prozent des Eurocard-Internetumsatzes).

¹² American Express verlangt die Angabe des sogenannten "Alphacodes", der als vierstellige Nummer auf der Vorderseite der American Express Card links neben der Kartennummer zu finden ist. Aus Sicherheitsgründen ist dieser Nummernteil nicht hochgeprägt wie die Kartennummer selbst.

Die Kreditkartendaten sind als besonders sensibel zu bewerten, da deren Angabe ausreichend ist, um Zahlungen zu tätigen. Auch die Kartenprüfnummer, die aus Sicherheitsgründen nicht im Magnetstreifen gespeichert wird und auch auf den Zahlungsquittungen nicht zu finden ist, muss über das Netz übertragen werden. Deshalb sollte hier die SSL-Verschlüsselung verwendet werden.

Die Kreditkartenzahlung im Internet mit SSL verläuft dabei wie folgt:

Ablauf der Kreditkartenzahlung mit SSL



Ablauf einer Kreditkartenzahlung im Internet mit SSL

1. Zahlungswunsch

Der Kunde wählt im Online-Angebot des Händlers die Kreditkartenzahlung mit SSL aus, um seine Zahlung zu tätigen.

2. Server-Authentifizierung

Der Kunde bekommt eine Bestätigung (Zertifikat) angezeigt, dass es sich um den Rechner des Händlers handelt.

3. Zahlungsaufforderung

Der Kunde wird aufgefordert seine Kreditkartendaten, d.h. seine Kreditkartennummer, den Namen des Kreditkarteninhabers und das Verfallsdatum, den Kreditkartentyp (z.B. Eurocard) sowie die Kartenprüfnummer (CVC-Code) anzugeben.

4. Verschlüsselte Kreditkartendaten

Der Kunde gibt seine Kreditkartendaten an und sobald er mit der Maus auf den Absende-Button klickt, werden diese verschlüsselt über das Internet an den Händler gesendet. Der Kunde bekommt die Bestätigung der Verschlüsselung seiner Daten in seinem Internet-Browser entsprechend angezeigt, beim Netscape Navigator beispielsweise durch das Schließen eines Schloßes. Erst beim Händler wird das Formular wieder zur Lesbarkeit entschlüsselt.

5. Bestätigung

Der Kunde erhält eine Bestätigung, dass der Händler die Kreditkartendaten empfangen hat.

6. Warenlieferung

Der Händler kann nun die Warenauslieferung in die Wege leiten.

7. Anfrage der Genehmigungsnummer

Der Händler druckt die Kreditkartendaten (Belege) aus und ruft sodann die Kreditkartengesellschaft/Acquirer an, um eine Genehmigungsnummer zu erhalten.

8. Versendung des Belegs

Die zugeteilte Genehmigungsnummer und der Vermerk „Mailorder“ (für MOTO-Vertrag) notiert er auf den Beleg und sendet diesen per Post/Fax der Kreditkartengesellschaft/Acquirer zu.

9. Gutschrift auf das Girokonto

Die Kreditkartengesellschaft/Acquirer überweist den Zahlungsbetrag auf das Girokonto des Händlers, abzüglich eines Disagios.

10. Belastung des Girokontos

Im Gegenzug belastet die Kreditkartengesellschaft/Acquirer das Konto des Kunden mit dem Zahlungsbetrag.

Wie auch beim Lastschriftverfahren ist hier die Voraussetzung zum Einsatz von SSL, dass der Kunde einen SSL-fähigen Internet-Browser benutzt und der Internet-Server des Händlers SSL unterstützt. Für die Server-Authentifi-

**Voraussetzungen
für SSL**

zierung benötigt der Händler zudem ein in der Regel kostenpflichtiges Zertifikat, welches die Identität seines Internet-Servers bestätigt.

Außerdem muss – wie bereits erwähnt – der Händler einen MOTO-Vertrag mit der jeweiligen Kreditkartengesellschaft/Acquirer abschließen.

Hoher Aufwand bei manueller Einreichung

Der Aufwand, jede Kreditkartenzahlung bei der Kreditkartengesellschaft/Acquirer manuell einzureichen, ist sehr hoch. Hinzu kommt das Risiko, dass nicht online geprüft wird, ob die Kreditkartendaten stimmen oder die Kreditkarte gesperrt ist. Rationeller und sicherer ist die Abwicklung der Kreditkartenzahlung im Internet über eine direkte Anbindung an den Rechner einer Autorisierungsstelle. Während einer Transaktion werden hierbei die Kreditkartendaten im Hintergrund auf Richtigkeit und Gültigkeit geprüft, um dann die Zahlung automatisch zu buchen. Der Händler erhält lediglich einen Report über die getätigten Zahlungen und eine Gutschrift auf sein Girokonto.

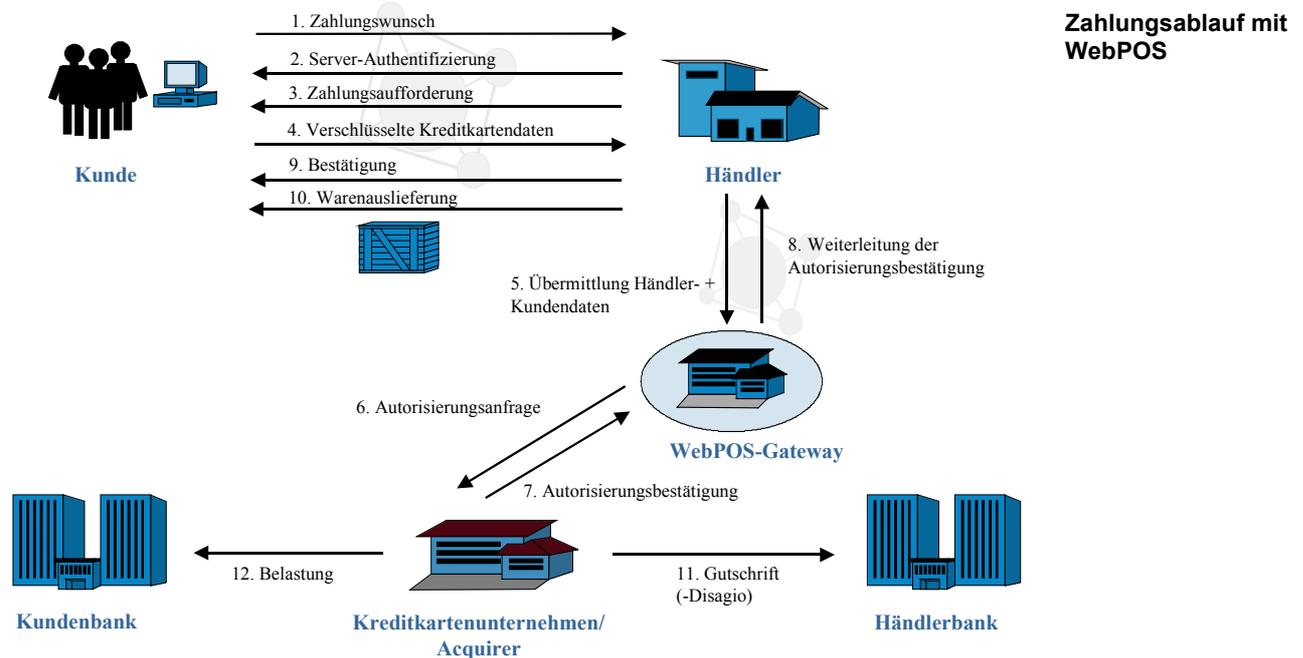
Es gibt eine Reihe von Dienstleistern/Systeme, die eine solche Anbindung für Kreditkartenzahlungen im Internet anbieten. Im folgenden Abschnitt wird als Beispiel das WebPOS-System dargestellt.

2.2.2 Kreditkartenzahlungen mit WebPOS

WebPOS¹³ ist das Internet-Kreditkartenzahlungssystem der Firma CyberCash Inc. und wird in Deutschland von mehreren Banken (u.a. Commerzbank, Dresdner Bank, HypoVereinsbank, Landesbank Baden-Württemberg, Landesbank Sachsen, Stadtparkasse Köln, Westdeutschen Landesbank) angeboten. Diese Banken werden im Weiteren als WebPOS-Banken bezeichnet.

Beim WebPOS-System liegt die Sicherung der Kundenanbindung ausschließlich beim Händler. Bei der folgenden Beschreibung des Zahlungsablaufs gehen wir davon aus, dass der Händler auf seinem Web-Server für die Verschlüsselung der Kreditkartendaten des Kunden SSL verwendet.

¹³ WebPOS ist das Nachfolgeprodukt von CyberCash, das im Dezember 2000 offiziell von der CyberCash Inc. eingestellt worden ist. Während CyberCash drei Internet-Zahlungssysteme unter einer einheitlichen Benutzungsoberfläche anbot, unterstützt WebPOS nur die Kreditkartenzahlung.



Zahlungsablauf einer Kreditkartenzahlung im Internet mit WebPOS

1. Zahlungswunsch

Der Kunde wählt im Online-Angebot des Händlers die Kreditkartenzahlung über WebPOS aus, um seine Zahlung zu tätigen.

2. Server-Authentifizierung

Der Kunde bekommt eine Bestätigung (Zertifikat) angezeigt, dass es sich um den Rechner des Händlers handelt.

3. Zahlungsaufforderung

Der Kunde wird aufgefordert, seine Kreditkartendaten, d.h. seine Kreditkartennummer, den Namen des Kreditkarteninhabers, das Verfallsdatum, den Kreditkartentyp (z.B. Eurocard) sowie die Kartenprüfnummer (CVC-Code) anzugeben.

4. Verschlüsselte Kreditkartendaten

Der Kunde gibt seine Kreditkartendaten an und sobald er mit der Maus auf den Absende-Button klickt, werden diese verschlüsselt über das Internet an den Händler gesendet. Der Kunde bekommt die Bestätigung der Verschlüsselung seiner Daten in seinem Internet-Browser entsprechend angezeigt,

beim Netscape Navigator beispielsweise durch das Schließen eines Schlosses. Erst beim Händler werden die Kreditkartendaten entschlüsselt.

5. Übermittlung von Händler- und Kundendaten

Die beim Händler eingesetzte WebPOS-Software fügt den übermittelten Kreditkartendaten die Händlerdaten, wie zum Beispiel die Händlerkennung, hinzu und überträgt diese wiederum verschlüsselt an das WebPOS-Gateway der CyberCash Inc. weiter. Das Gateway überprüft, ob die Händlerangaben korrekt und die Kundendaten vollständig sind; falls das nicht der Fall ist, wird der Vorgang abgebrochen.

6. Autorisierungsanfrage

Das WebPOS-Gateway fügt den Händler- und Kundendaten weitere Daten hinzu, wie zum Beispiel die VU-Nummer des Händlers, und übermittelt diese zur Autorisierung an das Kreditkartenunternehmen/Acquirer. Die Autorisierungsanfrage wird hierbei über das Bankennetzwerk gesendet, das auch für herkömmliche Kreditkartenzahlungen genutzt wird.

7. Autorisierungsbestätigung

Falls die Kartenprüfsumme richtig ist, die Kreditkarte weder abgelaufen, gesperrt oder ungültig ist und der Händler einen gültigen Vertrag mit dem Kreditkartenunternehmen hat, erfolgt die Autorisierung an das WebPOS-Gateway.

8. Weiterleitung der Autorisierungsbestätigung

Das Web-POS-Gateway leitet die Bestätigung per SSL an den Händler weiter.

9. Bestätigung

Der Kunde erhält eine Bestätigung, dass die Zahlung durchgeführt wurde.

10. Warenlieferung

Der Händler kann nun die Warenauslieferung in die Wege leiten.

11. Gutschrift auf das Girokonto

Die Kreditkartengesellschaft/Acquirer überweist den Zahlungsbetrag auf das Girokonto des Händlers, abzüglich eines Disagios.

12. Belastung des Girokontos

Im Gegenzug belastet die Kreditkartengesellschaft/Acquirer das Konto des Kunden mit dem Zahlungsbetrag¹⁴.

Voraussetzungen

Für eine Online-Anbindung an das WebPOS-System muss der *Händler* neben der SSL-Unterstützung und dem Abschluss eines MOTO-Vertrag, folgende Voraussetzungen erfüllen:

- **Händler-Vertrag**

Der Händler muss einen Händler-Vertrag für den WebPOS-Service mit einer WebPOS-Bank abschließen. Dabei muss der Händler bei dieser Bank auch ein Girokonto besitzen, über welches die Zahlungen mit WebPOS abgewickelt werden. Außerdem darf der MOTO-Vertrag nur mit bestimmten Acquireern, die dem WebPOS-Gateway einen Zugang für Autorisierungsanfragen erlauben, abgeschlossen werden. Der Vertrag kann zum Ende eines Kalendermonats gekündigt werden.

Voraussetzungen für den Händler

- **Integration des WebPOS-Services**

Dem Händler wird von der WebPOS-Bank ein Skript (Hilfsprogramm) zur Verfügung gestellt, welches vom Händler angepasst und in die Shop-Seiten integriert werden muss. Die Funktion des Skripts besteht darin, die Kreditkartendaten des Kunden zu übernehmen und an das WebPOS-Gateway weiterzuleiten.

Kosten

Die folgende Aufstellung der Händlerkosten für WebPOS entstammen dem Händlervertrag für den WebPOS-Service der Dresdner Bank (Stand November 2000). Diese Kosten entstehen dem Händler zusätzlich zu den Kosten für die Kreditkartentransaktionen laut MOTO-Vertrag sowie für die SSL-Verschlüsselung.

Kosten für den Händler

¹⁴ Der Händler kann über WebPOS die Belastung des Kreditkartenkontos des Kunden hinauszögern, um zu vermeiden, dass die Abbuchung des Zahlungsbetrages vor der Warenlieferung erfolgt.

Kosten für den *Händler*:

Entgelt für die Freischaltung des WebPOS-Services (einmalig)	50,- Euro
Abnahme der Shop-Integration (optional)	75,- Euro pro Abnahme
Kosten pro Transaktion ¹⁵	0,10 Euro pro Transaktion
Monatliches Mindest-Transaktionsentgelt	20,- Euro
Änderung von Händlerdaten	10,- Euro

2.2.3 Kreditkartenzahlungen mit SET

Bei den bisher beschriebenen Systemen für Kreditkartenzahlungen im Internet erfolgt keine ausreichende Überprüfung, ob auch wirklich der rechtmäßige Besitzer die Kreditkartendaten benutzt oder ein unbefugter Dritter. Für den Händler ist damit jede über die Kreditkarte abgewickelte Internet-Zahlung zunächst einmal ein unsicheres Geschäft, da die Beweislast und somit das Risiko auf seiner Seite liegt. Ein Widerspruch des Karteninhabers kann bei ihm mit hohen Aufwänden und Kosten verbunden sein.

Im Vergleich zur herkömmlichen Kreditkartenzahlung im Ladengeschäft mit persönlichem Kontakt und Unterschrift stellt bei den Kreditkartenzahlungen im Internet die nachweisbare Identifikation der Beteiligten (insbesondere des Kunden) sowie die Zahlungszustimmung des Kunden durch seine Unterschrift das Grundproblem da. Die Kreditkartenzahlungen sollen mit der SET (Secure Electronic Transaction)-Technologie auf das Medium Internet umgesetzt werden. Die Zahlungen im Internet können dann den herkömmlichen Kreditkartenzahlungen im Ladengeschäft rechtlich gleichgestellt werden. Insbesondere erhält der Händler bei SET von seiner Händlerbank eine vollständige Zahlungsgarantie.

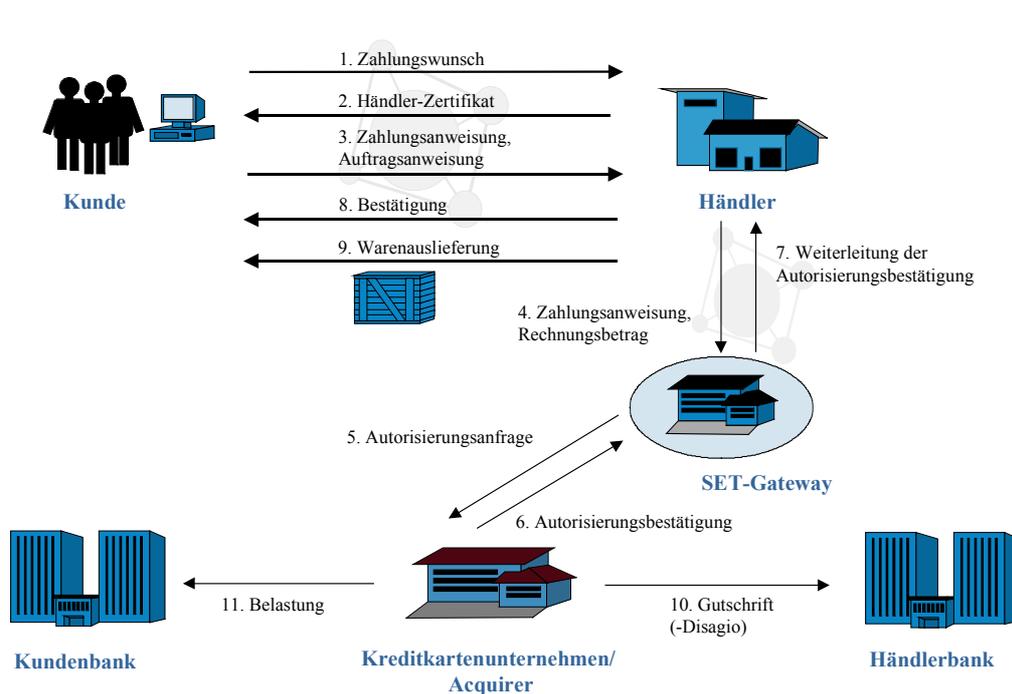
Die nachweisbare Identifikation der Beteiligten wird dadurch erreicht, dass sowohl der Karteninhaber (Kunde) als auch der Händler ein SET-Zertifikat erhalten, über welches sie sich bei einer Kreditkartenzahlung gegenseitig

¹⁵ Eine Transaktion ist hierbei einer Autorisierungsanfrage gleichgesetzt. Jede Autorisierungsanfrage an das WebPOS-Gateway kostet also 0,10 Euro, unabhängig davon, ob die Autorisierung erfolgreich war oder abgelehnt wurde.

ausweisen. Als besonderer Vorteil bleiben bei SET die Kreditkartendaten des Kunden dem Händler gegenüber verborgen. Dies stellt im Vergleich zu den herkömmlichen Kreditkartenzahlungen einen erheblichen Fortschritt dar und trägt dem Bedürfnis des Kunden nach Sicherheit und Privatsphäre Rechnung.

SET wurde von den Kreditkartenfirmen VISA und MasterCard zusammen mit den IT-Unternehmen IBM, Netscape, Microsoft, HP/Verifone, etc. entwickelt. Vermarktet wird das System durch die von VISA und MasterCard 1997 gegründete Firma "SET Secure Electronic Transaction LLC" (kurz: SETCo). SETCo koordiniert auch die im Umfeld von SET verteilten durchgeführten Entwicklungsarbeiten. Über die Homepage von SETCo (www.setco.org) können der aktuelle Stand sowie die Spezifikationen von SET abgerufen werden.

Die folgende Abbildung zeigt den Ablauf einer SET-Zahlung. Es sei angenommen, dass die vorher notwendigen Zertifizierungen der Beteiligten bereits erfolgt sind.



Zahlungsablauf einer Kreditkartenzahlung mit SET

1. Zahlungswunsch

Der Kunde leitet die SET-Zahlung mit einer Kaufanfrage ein und wählt als Bezahlungsart die Kreditkartenzahlung mit SET.

2. Händler-Zertifikat

Der Händler übergibt dem Kunden als Antwort auf die Kaufanfrage das Händler-Zertifikat und weitere für eine SET-Transaktion notwendigen Sicherheitsparameter.

3. Zahlungsanweisung, Auftragsanweisung

Der Kunde prüft das Händler-Zertifikat und sendet dem Händler eine Zahlungsanweisung (a) mit den Kreditkartendaten und eine Auftragsanweisung (b) mit den Bestelldaten. In beiden Anweisungen (a + b) ist das Zertifikat des Kunden enthalten.

4. Zahlungsanweisung, Rechnungsbetrag

Der Händler prüft die Auftragsanweisung des Kunden und dessen Zertifikat. Die Zahlungsanweisung bleibt verschlüsselt, so dass die Kreditkartendaten für den Händler nicht einsehbar sind. Der Händler sendet nun die verschlüsselte Zahlungsanweisung des Kunden zusammen mit dem Rechnungsbetrag und seinem Händler-Zertifikat gesichert an das SET-Gateway. Außer dem Rechnungsbetrag verbleiben die Bestelldaten beim Händler und bleiben im weiteren Verlauf den Kreditkartengesellschaften, Acquirer und Banken verborgen¹⁶.

5. Autorisierungsanfrage

Nachdem das SET-Gateway die Übereinstimmung der Zahlungsanweisung des Kunden mit dem Rechnungsbetrag des Händlers sowie die jeweiligen Zertifikate kontrolliert hat, werden die Kreditkartendaten zusammen mit dem Rechnungsbetrag zur Autorisierung an die Kreditkartengesellschaft/Acquirer weitergeleitet. Die Autorisierungsanfrage wird hierbei über das Bankennetzwerk gesendet, das auch für herkömmliche Kreditkarten-zahlungen genutzt wird.

¹⁶ Das Verbergen der Kreditkartendaten vor dem Händler einerseits sowie der Bestelldaten vor der Kreditkartengesellschaft, dem Acquirer und den Banken andererseits wird in SET durch die sogenannte duale Signatur realisiert.

6. Autorisierungsbestätigung

Falls die Daten richtig sind, d.h. die Kreditkarte weder abgelaufen, gesperrt oder ungültig ist und der Händler einen gültigen Vertrag mit dem Kreditkartenunternehmen hat, erfolgt die Autorisierung an das SET-Gateway.

7. Weiterleitung der Autorisierungsbestätigung

Das SET-Gateway leitet die Bestätigung an den Händler weiter.

8. Bestätigung

Der Kunde erhält eine Bestätigung, dass die Zahlung erfolgreich durchgeführt wurde.

9. Warenlieferung

Der Händler kann nun die Warenauslieferung in die Wege leiten.

10. Gutschrift auf das Girokonto

Die Kreditkartengesellschaft/Acquirer überweist den Zahlungsbetrag auf das Girokonto des Händlers, abzüglich des Disagios.

11. Belastung des Girokontos

Im Gegenzug belastet die Kreditkartengesellschaft/Acquirer das Konto des Kunden mit dem Zahlungsbetrag.

Voraussetzungen

Die für SET notwendigen Zertifikate werden von den jeweils zuständigen Banken ausgegeben, also im Falle des Karteninhabers von der Kundenbank, im Falle des Händlers von der Händlerbank.

Der *Kunde* benötigt darüber hinaus einen "SET-tauglichen" Browser. Dahinter verbirgt sich ein Plug-In (Softwaremodul), welches eine elektronische Brieftasche (Wallet) auf dem Kunden-PC realisiert. In dieser befindet sich das für SET zugelassene und registrierte Zertifikat sowie die zertifizierten Kreditkartendaten des Kunden. Die Wallet selbst ist passwortgeschützt.

**Voraussetzungen
für den Kunden**

Um SET-Bezahlungen als in-House-Lösung anbieten zu können, muss der *Händler* eine SET-Händlersoftware auf seinem Server installieren, welche SET-Transaktionen vom Kunden entgegennimmt und an das SET-Gateway weiterleitet. Eine SET-Händlersoftware wird von mehreren Herstellern angeboten, wobei hier zu beachten ist, dass es sich um eine SET-zertifizierte Lö-

**Voraussetzungen
für den Händler**

sung handelt. Dies bedeutet, dass es sich bei dieser SET-Lösung um eine von der SETCo abgenommenen Software handelt. Nur so kann die reibungslose Zusammenarbeit mit anderen SET-Komponenten, wie zum Beispiel der SET-Wallet des Kunden sichergestellt werden. Wichtig ist außerdem, dass die Software den aktuellen SET-Standard unterstützt. Der Händler benötigt zudem eine Online-Anbindung an das SET-Gateway.

Gehostete SET-Lösung

Insgesamt sind die Aufwände einer SET-Integration beträchtlich, da es sich bei SET um ein Hochsicherheits-Zahlungssystem für die Internet-Kreditkartenzahlungen handelt. Kleineren und mittleren Unternehmen ist daher eine gehostete SET-Lösung zu empfehlen: Das SET-System wird von einem Dienstleister betrieben, Installations- und Konfigurationaufgaben sowie die Bereitstellung der Sicherheitsinfrastruktur müssen nicht vom Händler selbst geleistet werden.

Kosten

Beispielhaft sei hier das SET-Hostingangebot der Berliner Sparkasse (Stand 18.04.2001) aufgeführt:

Kostenbeispiel gehostete SET-Lösung

Einrichtungspreis inkl. SET-Händlersoftware (einmalig)	1.190,- DM
SET Händlerzertifikat pro Jahr	250,- DM für VISA 250,- DM für Eurocard/MasterCard
Monatliche Miete für die SET-Hostinglösung (Vertragslaufzeit 24 Monate)	79,- DM
Transaktionspreis je Kreditkartenumsatz mittels SET	0,10 DM
Disagio (Bearbeitungs-/Garantiegebühr der Kreditkartengesellschaft)	3,5 % vom Umsatz
Stornogebühr	jeweils 2,50 DM
Chargebackgebühr (Widerspruch durch Karteninhaber)	jeweils 35,- DM

(Quelle: Betreuungszentrum Electronic Banking Berliner Sparkasse, [http://www.berliner-sparkasse.de/bsk/pui.nsf/ViewFileDownload/ecomms.pdf/\\$File/ecomms.pdf](http://www.berliner-sparkasse.de/bsk/pui.nsf/ViewFileDownload/ecomms.pdf/$File/ecomms.pdf))

Kostenbeispiel: SET als Shop-in-a-Box-Lösung

Das Angebot bezieht sich auf die Integration von SET in einen vorhandenen Internet-Shop. Bei geringen Umsätzen kann hier eine vollintegrierte Lösung

günstiger sein, also das Anmieten eines Shopsystems mit integrierter SET-Zahlungslösung.

Verkauf von Einzelprodukten über statische Web-Seiten:

- einmalig: 149,00 DM
- je Produkt: 15,00 DM
- je Transaktion: 0,35 DM

Verkauf aus Katalog, also einem Internet-Shop mit einer Katalog-Datenbank und einem Warenkorbsystem:

- einmalig ab: 379,00 DM
- monatlich: 19,00 DM
- je Transaktion: 0,35 DM

Quelle: Volksbank Dreieich eG: http://www.vobadreieich.de/firmenpark/assistenten/info_shopinbox.cfm, Stand 6. Juni 2001)

SET setzt eine relativ komplexe technische und organisatorische Infrastruktur voraus, weshalb bislang nur sehr wenige Händler SET-Zahlungen anbieten. Trotzdem bestehen sehr gute Chancen, dass SET sich als Standard für Kreditkartenzahlungen durchsetzen wird. Diese Sicht stützt sich auf folgende Punkte:

- SET ist die Internet-gerechte Umsetzung eines Zahlungssystems (Kreditkarte), das sich als internationales Zahlungsmittel mit allgemeiner Akzeptanz etabliert hat.
- SET bietet dem Kunden den höchsten Grad an Anonymität, der sich mit einem Kreditkartenzahlungssystem erreichen lässt.
- Die Entwicklung von SET wird koordiniert und konsequent vorangetrieben. So sollen mit SET auch Chipkarten und elektronische Geldbörsen unterstützt werden, über die zusätzlich Zahlungen von Kleinstbeträgen möglich sein wird. Außerdem sollen E-Banking und E-Payment sowohl im Internet als auch im Mobilfunknetz zu einem durchgängigen Konzept verschmolzen werden. Grundlage hierfür ist ein Drei-Domänen-Modell für SET (3D-SET) das eine flexible Zuordnung von Verantwortlichkeiten erlaubt.
- SET erfährt national und international eine breite Unterstützung durch Banken und Finanzinstitute.
- Die Kreditkartengesellschaften forcieren SET, um die Kreditkarte als Standard-Bezahlmethode im Internet zu etablieren. So gibt Visa seit dem 1. Juni 2001 jedem Händler, der SET einsetzt, eine Zahlungsgarantie,

**Bewertung und
Perspektiven von
SET**

3D-SET

auch dann, wenn der Kunde kein SET-Zertifikat zur Identifizierung benutzen kann oder will.

2.3 GeldKarte

Die GeldKarte¹⁷ ist ein Wert-basiertes Zahlungssystem, bei welchem vor der Bezahlung digitales Geld auf die Chipkarte geladen wird. Der Benutzer einer Geldkarte tauscht also konventionelles Geld in eine elektronische Form von Geld um. Als elektronische Geldbörse soll die Geldkarte Münzen und Scheine ersetzen und zur Begleichung kleinerer Beträge im Einzelhandel, an Automaten (mit Getränken, Süßigkeiten usw.), an Parkuhren oder auch beim Lösen einer Busfahrkarte dienen. Seit Mai 1999 kann sie auch zum Bezahlen im Internet genutzt werden.

Eingeführt durch
Zentralen Kredit-
ausschuss

Die Geldkarte wurde vom Zentralen Kreditausschusses (ZKA) eingeführt, an dem neben dem Deutschen Sparkassen- und Giroverband der Bundesverband der Deutschen Volksbanken und Raiffeisenbanken, der Bundesverband Öffentlicher Banken Deutschlands sowie der Verband Deutscher Hypothekenbanken beteiligt ist.

Seit 1996 befindet sich die Geldkarte als kleiner goldener Chip auf den Kunden- bzw. EC-Karten und steht damit als Zahlungssystem inzwischen über 50 Millionen EC-Kartenbesitzern in Deutschland zur Verfügung. Diese Art der Karten bezeichnet man als kontogebundene Karte, da sie einen Bezug zu einem Girokonto besitzen.

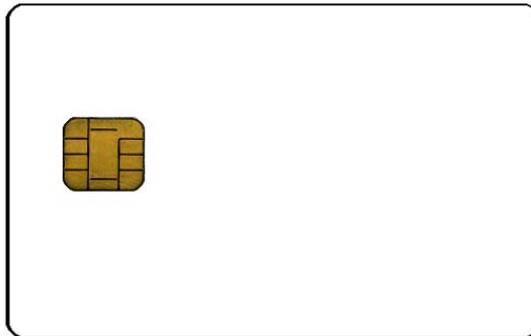


Beispiel einer kontogebundenen Geldkarte

¹⁷ Statt des Markennamens 'GeldKarte' werden wir die gefälligere Schreibweise 'Geldkarte' verwenden.

Die Geldkarte kann aber auch als eigenständiges Bezahlssystem unabhängig von einem Konto eingesetzt werden. Bei kontounterbundenen Karten befindet sich der Börsen-Chip auf sogenannten "weißen" Karten. Diese haben keinen Bezug zu einem Konto und machen daher anonyme Zahlungen möglich. Kontounterbundene Geldkarten können - wie Telefonkarten - käuflich erworben werden.

Weißer Karten



Kontounterbundene Geldkarte

Um mit einer Geldkarte bezahlen zu können, muss sie geladen sein. Der Geldbetrag wird im Chip der Karte gespeichert und ist derzeit auf 400,- DM begrenzt. Geldkarten können jederzeit erneut bis zu diesem Höchstbetrag aufgeladen werden.

Das Aufladen der Geldkarte geschieht entweder an einem Geldkarten-Ladeterminale unter Eingabe der PIN (ähnlich wie beim Geldabheben am Automaten) oder gegen Barzahlung in einer Bankfiliale. In Zukunft soll auch das Aufladen über das Internet als Funktion des Homebankings nach dem HBCI-Standard (Home Banking Computer Interface) möglich sein. Nach dem Ladevorgang befindet sich der gewünschte Betrag auf dem Chip der Geldkarte und steht zum Einkaufen zur Verfügung.

Für jede Geldkarte wird ein Schattenkonto mit dem aktuellen Kartensaldo geführt. Ein Schattenkonto ist ein spezielles Konto, das nur für die systemtechnische Abwicklung der Zahlungsvorgänge verwendet wird und nach außen nicht in Erscheinung tritt. Mit dem Aufladen der Geldkarte wird der Saldo auf dem Schattenkonto um den Ladebetrag erhöht und bei einer Zahlung um den Zahlungsbetrag entsprechend vermindert. Über die Schattenkonten können die Geldflüsse nachvollzogen werden. Ist die Karte des Kunden defekt, so kann der aktuell auf dem Schattenkonto gespeicherte

Schattenkonto

Verfügungsbetrag dem Kunden wieder erstattet werden. Hierzu ist lediglich die Nummer der Geldkarte, aber nicht der Name des Kunden notwendig.¹⁸

Verbreitung der Geldkarte

Als elektronische Alternative für die Funktion des Bargeldes, insbesondere der Bezahlung von Kleinbeträgen, hat die Geldkarte ein weites Anwendungsfeld. Einen Überblick über aktuelle Pilotprojekte und Anwendungen finden Sie auf der Web-Site der SCARD Service GmbH (<http://www.scard.de/anwend/an.htm>). In vielen Orten ist es bereits möglich, in öffentlichen Verkehrsmittel und Parkhäusern mit der Geldkarte zu bezahlen (<http://finanzen.focus.de/D/DA/DAC/DAC31/DAC31D/dac31d.htm>).

Eine im Juni 2000 durchgeführte Händlerbefragung der SCARD Service GmbH zeigt jedoch - bei einer fast flächendeckenden Verbreitung der Geldkarte - die insgesamt mangelnde Kundenakzeptanz:

- In Deutschland sind 52 Millionen Karten mit Geldkarten-Funktion im Umlauf.
- Im September 2000 wurden ca. 2,2 Millionen Geldkarten-Transaktionen durchgeführt (Tendenz steigend, ca. 30% pro Jahr).
- Es existieren ca. 65.000 Geldkarten-Akzeptanzstellen (Tendenz gleichbleibend).
- Die durchschnittlichen Ladebeträge lagen im Jahr 2000 bei 60 DM, die durchschnittlichen Bezahlbeträge bei 5 DM (Tendenz fallend).

(Quelle: http://www.scard.de/news/geldkarte_statistik_1.htm)

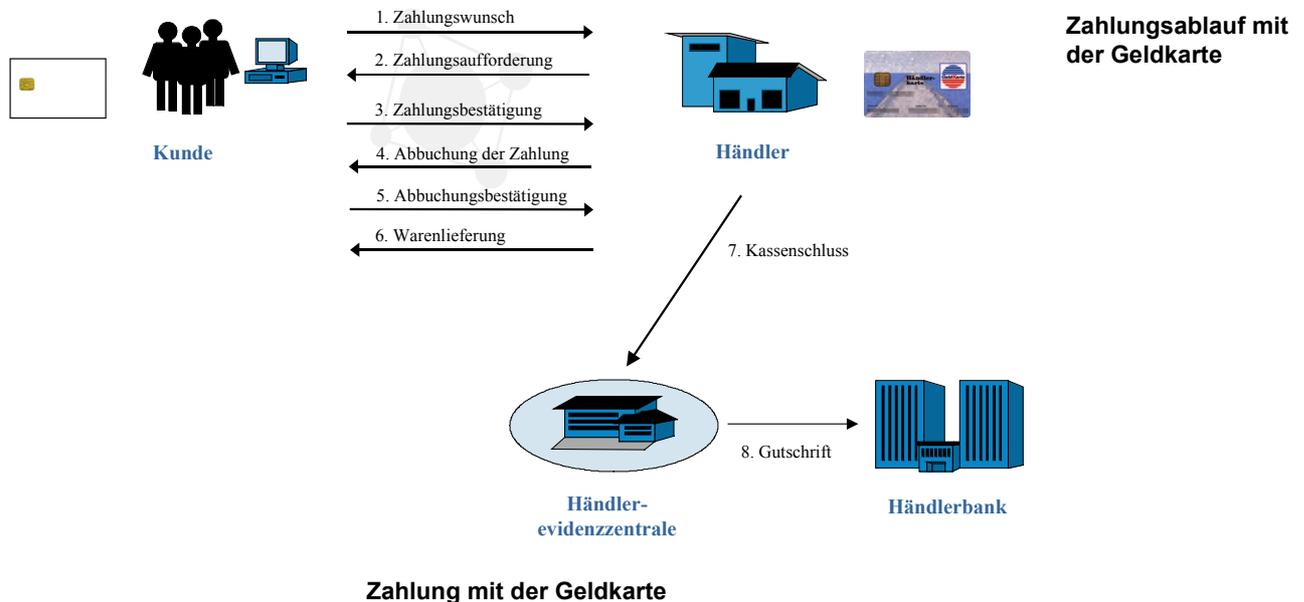
Teilnehmer

Bei der Zahlung mit der Geldkarte gibt es folgende Teilnehmer:

- den Kunden, welcher mit der Geldkarte seine Zahlung tätigt,
- den Händler, welcher die Geldkarte zur Zahlung in seinem Internet-Shop anbietet,
- die Geldkarten-Akzeptanzstelle, die Geldkarten-Zahlungen annimmt,
- die Händlerbank, die mit dem Händler einen Geldkarten-Vertrag schließt und dem Händler seine Händlerkarte ausstellt,
- die Händlerevidenzzentrale, welche die Zahlungstransaktionen prüft und die Beträge auf dem Händlerkonto gutschreibt,
- die Börsen- oder Kartenevidenzzentrale, die für jede Geldkarte ein Schattenkonto führt,

¹⁸ Bei Verlust der GeldKarte trägt der Kunde - wie bei verlorenem Bargeld auch - das Risiko. Er kann jedoch die Karte sperren lassen. Die dann auf dem Schattenkonto verbliebenen Beträge werden dem Kunden nicht gutgeschrieben, sondern von der Bank eingezogen.

- Die Verrechnungsbanken, die das Clearing, also den Ausgleich der kumulierten Geldbeträge über Verrechnungskonten durchführen.



1. Zahlungswunsch

Der Kunde hat seinen Warenkorb zusammengestellt und möchte bezahlen. Unter den angebotenen Bezahlverfahren wählt er die Geldkarte aus.

2. Zahlungsaufforderung

Im Internet-Browser des Kunden erscheint ein Fenster, das dem Kunden die Zahlungsdaten anzeigt.

3. Zahlungsbestätigung

Ist der Kunde mit dem Zahlungsvorgang einverstanden, bestätigt er per Mausklick den Zahlungsvorgang und legt seine Geldkarte in den Chipkartenleser. Die Karte wird gelesen und das auf der Karte verfügbare Guthaben angezeigt. Der Kunde bestätigt die Zahlung abschließend. Die Zahlungsdaten¹⁹ werden per SSL verschlüsselt an den Händler übertragen.

¹⁹ Zu diesen Daten gehören neben dem Guthaben der Karte weitere Identifikationsdaten, wie z.B. das Verfallsdatum. Außerdem sendet die Geldkarte einen Code, der durch die DES-Verschlüsselung einer Zufallszahl entstanden ist. Diese wurde aus der mit der Zahlungsaufforderung gesendeten Zufallszahl des Händlers gebildet. Durch dieses Verfahren kann die Echtheit der Kunden-Geldkarte sichergestellt werden.

4. Abbuchung des Zahlungsbetrages

Beim Händler (genauer: bei der Geldkarten-Akzeptanzstelle) wird die Echtheit der Kunden-Geldkarte anhand der Zahlungsdaten geprüft. Wird die Karte als echt akzeptiert, wird die Aufforderung zur Abbuchung des Zahlungsbetrags zum Kunden gesendet.

5. Abbuchungsbestätigung

Die Geldkarte des Kunden reduziert das aktuelle Guthaben um den Zahlungsbetrag. Im Browserfenster wird der neue aktuelle Ladebetrag der Geldkarte angezeigt. Der Inhalt des Fensters kann ausgedruckt als Quittung verwendet werden. Die Abbuchung wird abschließend dem Händler bestätigt.

6. Warenlieferung

Der Händler kann nun die Warenauslieferung in die Wege leiten.

7. Kassenschluss

Die Zahlungen werden in Form von Transaktionsdatensätze gesammelt und bei Kassenschluss des Händlers (in der Regel einmal am Tag) zur Händler-evidenzzentrale geschickt.

8. Gutschrift

In der Händlerevidenzzentrale werden die eingehenden Zahlungs- und Summensätze auf Doppeleinreichungen oder andere Unstimmigkeiten geprüft. Ist die Überprüfung erfolgreich abgeschlossen, wird auf das Händlerkonto eine Gutschrift über den Gesamtbetrag der eingereichten Transaktionsdatensätze (Händlersammelgutschrift) erzeugt. Über die Verrechnungsbank wird die Überweisung auf das Geschäftskonto des Händlers veranlasst. Die Händlerevidenzzentrale trennt die eingereichten Transaktionssätze nach den Bankleitzahlen und leitet sie weiter an die entsprechenden Börsenevidenzzentralen, die die zu den Geldkarten gehörenden Schattenkonten führen. Dort werden die Salden der den Geldkarten zugehörigen Schattenkonten entsprechend der Transaktionsbeträge herabgesetzt.

Voraussetzungen

Voraussetzungen für den Kunden

Damit der *Kunde* mit der Geldkarte im Internet bezahlen kann, muss er neben einer geladenen Geldkarten noch folgende Voraussetzungen erfüllen:

- Chipkartenleser

Der Kunde benötigt für seinen Rechner ein Chipkartenlesegerät der Klasse 3. Diese Geräte verfügen aus Sicherheitsgründen über eine eigene Tastatur und ein eigenes Display²⁰. Über das Display wird dem Kunden bei jedem Zugriff auf die Geldkarte der Zahlungsempfänger und der Abbuchungsbetrag angezeigt. Der Kunde muss dann die Angaben direkt an der Tastatur des Lesegerätes bestätigen. Auf diese Weise kann verhindert werden, dass in den Rechner eingeschleuste Hackersoftware (sogenannte 'trojanische Pferde') unbemerkt auf die Geldkarte des Kunden zugreift und Guthaben abbucht.

- Geldkarten-Software

Zum Auslesen, zum Bezahlen sowie zur Verwaltung der Geldkarte muss der Kunde eine Geldkarten-Software auf seinem Rechner installieren. Die Software kann bislang bei den Geldinstituten kostenlos heruntergeladen werden. So stellt beispielsweise das Informatikzentrum der Sparkassenorganisation die Geldkarten-Anwendung sowie die benötigten Treiber für die Chipkartenleser als Geldkarten-Starterkit online zur Verfügung (<http://ecommerce.sparkasse.de/>). Zugelassene Geldkarten-Software muss aus Sicherheitsgründen vom Zentralen Kreditausschuss zertifiziert sein.

- Javafähiger Internet-Browser

Der Internet-Browser des Kunden muss Java unterstützen, da die Zahlungsaufforderung in Form eines Java-Applets geladen wird.

Voraussetzungen für den *Händler*, um die Geldkarte in seinem Internet-Shop als Zahlungssystem anzubieten:

**Voraussetzungen
für den Händler**

- Girokonto

Der Händler benötigt ein Geschäftskonto bei einem Kreditinstitut (Händlerbank), das die Zahlung mit der Geldkarte unterstützt (zur Zeit Sparkassen, Raiffeisen- und Volksbanken oder Landesbank).

- Geldkarten-Vertrag

Der Händler schließt mit seiner Händlerbank einen Geldkarten-Vertrag, in welchem er sich unter anderem verpflichtet, nur Händlerterminals und Kar-

²⁰ Im November hat der zentrale Kreditkartenausschuss des Bankgewerbes den ersten Chipkartenleser („Kaan Professional“ der Firma Kobil) für den Einsatz der Geldkarte im Internet zertifiziert. Diese Geräte sind bislang mit 200,- DM in der Anschaffung relativ teuer. Lesegeräte der Klasse 3 sollen in Zukunft standardmäßig im Bankenumfeld eingesetzt werden, so dass sie dann auch für HBCI-Homebanking oder für die Verwendung der digitalen Unterschrift genutzt werden können. Vielleicht werden sie zukünftig von den Banken subventioniert.

tenlesegeräte einzusetzen, die den Vorgaben der Kreditwirtschaft entsprechen. Er erhält dann eine physische Händlerkarte sowie ein spezielles Geldkarten-Zertifikat, das ihn als legitimen Händler im Internet ausweist.



Beispiel einer physischen Händlerkarte

Alternativ hierzu kann er bei einer Geldkarten-Akzeptanzstelle den Einsatz einer virtuellen Händlerkarte beantragen, die insbesondere für das Massengeschäft geeignet ist, da mit ihr bis zu 10.000 Zugriffe gleichzeitig möglich sind.

- Service-Vertrag mit einer Geldkarten-Akzeptanzstelle

Der Händler schließt mit einer Geldkarten-Akzeptanzstelle einen Servicevertrag zur Abwicklung von Geldkarten-Zahlungen ab und überlässt der Akzeptanzstelle seine Händlerkarte. Geldkarten-Akzeptanzstellen sind in der Regel spezielle Dienstleistungsunternehmen wie z.B. Payment-Service-Provider.

- Geldkarten-Kassensystem

Der Händler betreibt in seinem Internet-Shop ein Kassensystem mit Geldkarten-Erweiterung, das dem Kunden die Bezahlung mit der Geldkarte ermöglicht. Über das Kassensystem werden die Zahlungstransaktionen an die Einkaufsprozesse im Internet-Shop gekoppelt. Das Kassensystem des Shops wiederum ist mit der Geldkarten-Akzeptanzstelle verbunden, bei welcher die Zahlungsbeträge dem Händler auf die Händlerkarte gutgeschrieben werden.

Der Betrieb der Geldkarten-Akzeptanz kann auch ohne Dienstleister durch den Händler selbst erfolgen. Einige Dienstleister für die Zahlungsabwicklung bieten hierfür bereits schlüsselfertige Lösungen an .

Eine aktuelle Liste der vom Zentralen Kreditausschuss zugelassenen Internet-Händlersysteme und Terminals für das Geldkarten-System finden Sie unter <http://www.voeb.de/Topics/gkv3.htm>.

Kosten

Die Kosten, die dem Händler und dem Kunden bei der Nutzung der Geldkarte entstehen, werden durch den Zentralen Kreditausschuss festgelegt.

Beim Bezahlen mit der Geldkarte entstehen dem Kunden keine Kosten. Ebenfalls keine Kosten entstehen für das Laden der Geldkarte über die Hausbank. Fremdinstitute berechnen für das Aufladen der Karte im allgemeinen 1,00 bis 2,00 DM.

Kosten für den Kunden

Die Autorisierungsgebühr der Kreditwirtschaft beträgt hier 0,3% vom Umsatz, mindestens aber DM 0,02. Für diesen Preis erhält der Händler eine 100%-tägige Zahlungsgarantie. Werden Dienstleister zur Geldkarten-Akzeptanz in Anspruch genommen, so fallen einmalige Kosten in Höhe von ca. 2000 DM sowie monatliche Kosten in Höhe von etwa 100 DM bis 200 DM an. Zusätzlich kann pro Transaktion eine weitere Gebühr (Einreichergebühr, typisch 0,05 DM) erhoben werden.

Kosten für den Händler

Bei der Eigenrealisierung der Geldkarten-Akzeptanz sind die Anschaffungskosten für die Geldkarten-Händlersoftware sowie die zertifizierten Karten-Lesegeräte anzusetzen.

Die Geldkarte hat das Potenzial, sich mittelfristig als Internet-Zahlungssystem zu etablieren.

Beurteilung und Perspektive

Positiv hervorzuheben sind

- die bequeme Zahlungsabwicklung für den Kunden: keine PIN, keine spezielle Autorisierung, eine Vielzahl von Lademöglichkeiten,
- die vergleichsweise geringen Transaktionskosten auf Händlerseite,
- die Zahlungsgarantie für den Händler,
- das hohe Maß an Sicherheit für Händler und Kunde,
- die hohe Verbreitung der Geldkarte,
- die Anonymität der Bezahlung,
- die Eignung für die Bezahlung kleinerer Beträge.

Das Hauptproblem für die Akzeptanz der Geldkarte als Internet-Zahlungssystem stellt zur Zeit die Notwendigkeit eines nicht gerade billigen Kartenlesers der Klasse 3 dar. Das könnte sich jedoch grundlegend ändern, wenn sich der Klasse-3-Leser zu einer multifunktionalen Standardkomponente am PC mausert, die neben der Geldkarten-Zahlung als Geldkarten-Ladeterminal,

für das HBCI-Homebanking und für die digitale Signaturen genutzt werden kann.

2.4 paybox

paybox zählt zu den Handy-basierten Zahlungssystemen. Anbieter ist hier die paybox.net AG, an welcher die Deutsche Bank mit 50% und die debitel AG seit September 2000 mit 4,8 Prozent beteiligt sind. Die übrigen Anteile liegen beim Vorstand und den Mitarbeitern des Unternehmens. Das paybox-System wurde im Mai 2000 am Markt eingeführt. Inzwischen bieten über 330 Händler im Internet die Bezahlung mit paybox an; von über 200.000 potentiellen Kunden kann diese Zahlungsart bereits genutzt werden (Stand Juni 2001). Zusätzlich ist paybox in den Ländern Spanien, Österreich und Schweden als Zahlungssystem verfügbar.

Es gibt verschiedene Varianten der bargeldlosen Bezahlung mit paybox. Prinzipiell kann zwischen folgenden Möglichkeiten unterschieden werden:

- internet-to-paybox, um mit dem Mobilfunktelefon Zahlungen im Internet anzuweisen,
- paybox-to-paybox, um Zahlungstransaktionen zwischen zwei privaten Mobilfunkteilnehmern durchzuführen,
- mobile-to-paybox, um mobile Dienstleistungen wie z.B. Taxi²¹, Pizzaservice, mit dem Handy zu begleichen, sowie
- POS-to-paybox, um im stationären Einzelhandel mit paybox zu zahlen.²²

Teilnehmer bei paybox

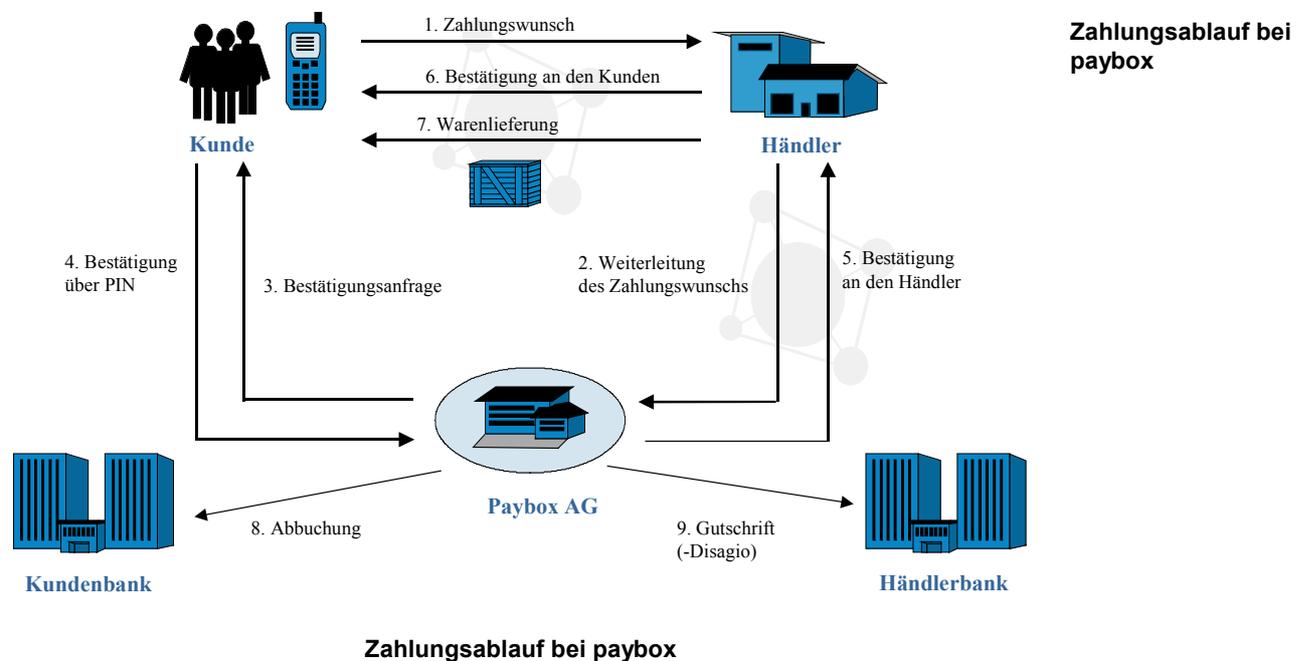
Bei dem Zahlungssystem paybox gibt es folgende Teilnehmer:

- den Kunden, der mit paybox seine Zahlung tätigt,
- den Händler, der paybox als Zahlungssystem anbietet,
- die paybox.net AG, welche die paybox-Zahlungen abwickelt, sowie
- die Deutsche Bank AG, welche die Abbuchung von dem Kundenkonto sowie die Wertstellung auf dem Händlerkonto realisiert.

²¹ Bislang bieten ca. 3600 Taxen das Bezahlen mit paybox an.

²² Hierzu sollen die Scanner-Kassen in Supermärkten die Handy- bzw. Aliasnummer des Kunden über einen Barcode-Leser einlesen, die dann an das paybox-System übermittelt wird (vergleiche Zahlungsablauf Paybox).

Der Zahlungsablauf bei paybox gestaltet sich wie folgt:



1. Zahlungswunsch

Nachdem der Kunde im Internet-Shop des Händlers seinen Warenkorb zusammengestellt hat, wählt er als Zahlungssystem paybox aus. Es erscheint eine Internetseite, auf welcher der Kunde seine Handynummer einträgt und die Zahlung per Mausklick bestätigt. Die Zahlungsdaten werden an den Händler übermittelt. Statt der Handynummer kann der Kunde auch eine Aliasnummer (eine siebenstellige paybox-Nummer, die nicht mit der Handynummer identisch ist), eintragen²³.

2. Weiterleitung des Zahlungswunsches

Eine auf Händlerseite installierte Software leitet den Zahlungswunsch des Kunden an die paybox.net AG weiter. Diese Übermittlung der Daten erfolgt über eine verschlüsselte SSL-Verbindung.

²³ Die Übertragung der Daten vom Kunden zum Händler erfolgt unverschlüsselt. Verwendet der Kunde seine Handynummer zur Zahlung und gelangt diese in die Hände Dritter, so könnten beispielsweise unerwünschte Werbe-SMS die Folge sein. Deshalb sollte der Händler für die Kundenanbindung zusätzlich eine SSL-Verschlüsselung einsetzen.

3. Bestätigungsanfrage

Die paybox.net AG prüft die Daten des Kunden und die des Händlers und ruft dann den Kunden auf dem Handy an. Der Kunde wird gefragt, ob er sich mit der Zahlung beim Händler einverstanden erklärt. Diese Anfrage erfolgt durch eine automatisch generierte Stimme.

4. Bestätigung durch die PIN

Der Kunde bestätigt die Zahlung mit Eingabe seiner persönlichen paybox-PIN. Sollte der Kunde mit der Zahlung nicht einverstanden sein, kann er mittels entsprechender Eingabe am Handy die Zahlung ablehnen.

5. Bestätigung an den Händler

Ist die Zahlung durch die korrekte PIN-Eingabe gegenüber der paybox.net AG bestätigt, übermittelt die paybox.net AG eine Bestätigung an den Händler.

6. Bestätigung an den Kunden

Der Kunde erhält eine Bestätigung über die erfolgte Zahlung zum einen vom Händler über das Internet und zum anderen von der paybox.net AG per SMS. Die Gesamtdauer des Zahlungsablaufs beträgt ca. 50 Sekunden.

7. Warenlieferung

Der Händler kann nun die Warenauslieferung in die Wege leiten.

8. Abbuchung beim Kundenkonto

Die paybox.net AG reicht bei der Deutschen Bank eine Lastschrift ein, welche den Betrag vom Girokonto des Kunden einzieht.

9. Gutschrift auf das Händlerkonto

Der Zahlungsbetrag wird dem Händler unter Abzug eines Disagios auf sein Händlerkonto bei der paybox.net AG gutgeschrieben. Der Saldo wird alle 14 Tage über die Deutsche Bank AG auf das Girokonto des Händlers überwiesen.

Voraussetzungen

**Voraussetzungen
des Kunden**

Damit der *Kunde* mit paybox zahlen kann, muss er zuvor folgende Voraussetzungen erfüllen:

- Mobiltelefon mit gültiger SIM-Karte

Der Kunde muss Besitzer eines Mobiltelefons mit gültiger Karte sein. An das Handy sind keine weiteren Bedingungen geknüpft. Es ist gleichgültig, von welchem Hersteller das Mobiltelefon stammt, welches Mobilnetz der Kunde verwendet und ob es sich um eine Karte mit Festvertrag oder um eine Pre-paid-Karte handelt.

- Vertrag mit der paybox.net AG (Endkunden-Vertrag)

Der Kunde muss mit der paybox.net AG einen Endkunden-Vertrag abschließen, der die Volljährigkeit des Kunden voraussetzt. Neben der Angabe persönlicher Daten stimmt der Kunde im Vertrag einer Bonitätsprüfung und einer Einzugsermächtigung für sein Girokonto für alle mit paybox getätigten Zahlungen zu. Den Zahlungen kann der Kunde sechs Wochen lang widersprechen, da diese über das Lastschriftverfahren eingezogen werden. Der Vertrag kann jederzeit ohne Einhaltung einer Frist gekündigt werden. Nach der Vertragsschließung erhält der Kunde seine persönliche 4-stellige paybox-PIN, mit welcher er seine Zahlungen über das Handy bestätigt.

Dem *Händler* werden drei grundlegende Varianten zur Integration von paybox in seinen Internet-Shop angeboten:

**Voraussetzungen
des Händlers**

- Der Basic Service basiert auf einer gehosteten Lösung und benutzt das Verfahren der 'Online-Autorisierung mit manueller Freigabe'. Der Kunde wird bei der Wahl des Zahlungssystems paybox auf einen Server der paybox.net AG umgeleitet. Dort gibt der Kunde seine Handy- bzw. Aliasnummer ein und die Zahlung wird, wie oben beschrieben, abgewickelt. Der Händler wird unabhängig von einzelnen Kundenzahlungen per E-Mail oder SMS benachrichtigt. Den Einzug des Zahlungsbetrages vom Girokonto des Kunden muss der Händler bei der paybox.net AG explizit anfordern.
- Der Standard Service bietet weitergehende Möglichkeiten zur Automatisierung und Integration der Zahlungsprozesse in die Systemumgebung des Händlers als der Basic Service. So erfährt der Händler direkt während der Zahlung, ob diese erfolgreich abgewickelt wurde oder nicht (Verfahren der 'Online-Autorisierung mit automatischer Freigabe'). An diese Freigabe kann er dann die Lieferung seiner Ware koppeln²⁴. Zusätzlich wird dem Händler ein elektronischer Transaktionsbericht zur internen Weiterbearbeitung (z.B. zur Erstellung von Berichten) zur Verfügung gestellt. Der Standard Service ist mit der Installation der paybox-

**Elektronischer
Transaktionsbe-
richt**

²⁴ Dies ist vor allem bei digitalen Gütern wie Musik oder Informationen wichtig.

Software auf den Internet-Server des Händlers verbunden. Die Anbindung des Internet-Shops an das Zahlungssystem erfolgt durch mitgelieferte Skripte (Hilfsprogramme), die auf die Systemumgebung des Händlers anzupassen sind.

Anbindung an die Logistik

- Der Premium Service ist für große Unternehmen entwickelt worden und bietet weitergehende Möglichkeiten zur Integration in die unternehmensspezifischen Geschäftsprozesse an als der Standard-Service.

Zusätzlich zur Online-Autorisierung mit integrierter Freigabe ermöglicht er eine automatisierte Anbindung an die Logistik über Datei- und XML-Schnittstellen.

In allen Fällen muss der Händler mit der paybox.net AG zwei Verträge abschließen, einen Dienstleistungsvertrag und einen Softwarelizenzvertrag. Die Vertragszeiten belaufen sich auf 6 Monate beim Basic Service, beim Standard und Premium Service auf 12 Monaten.

Kosten

Die folgende Aufstellung der Kosten, die dem Händler und dem Kunden bei der Nutzung von paybox entstehen, entstammen den Preislisten der paybox.net AG, Stand Mai 2001.

Kosten für den Kunden

Jährliche Grundgebühr	5,- Euro im Jahr
Änderung der Paybox-Nummer	15,- Euro

Roaming-Gebühren, die durch den Anruf der paybox.net AG entstehen, wenn der Kunde sich zu dieser Zeit außerhalb seines Mobilfunknetzes befindet, muss der Kunde tragen.

Kosten für den Händler

Die Kosten richten sich nach der vom Händler gewünschtem paybox-Serviceklasse:

Kosten für den paybox Basic Service:

Lizenzgebühren für die Händler- software	250 Euro
Jahresgebühr	100,- Euro
Kosten pro Transaktion	5% des Bruttobetrag
Kosten pro Storno	0,25 Euro
Kosten pro Gutschrift	3 Euro

Kosten für den paybox Standard Service:

Lizenzgebühren für die Händler- software	500,- Euro
Jahresgebühr	100,- Euro
Kosten pro Transaktion	3,5% des Bruttobetrag
Kosten pro Storno	0,25 Euro
Kosten pro Gutschrift	3 Euro

Kosten für den paybox Premium Service:

Lizenzgebühren für die Händler- software	2500,- Euro
Jahresgebühr	300,- Euro
Kosten pro Transaktion	3% des Bruttobetrag
Kosten pro Storno	0,25 Euro
Kosten pro Gutschrift	3 Euro

2.5 net900 Classic

net900 ist ein von der Firma "in medias res" patentiertes Zahlungssystem für das Internet und wird über sogenannte net900-Anbieter, wie z.B. die Firma Isoft GmbH, vertrieben. Die Deutsche Telekom hat net900 lizenziert und bietet dieses unter dem Namen „click&pay Net900“ im T-Online-Bereich an. Mittlerweile gibt es viele Zahlungssysteme wie z.B. X-Diver oder infin Micro-payment, die ähnlich wie net900 funktionieren und sich nur in Details unterscheiden.

**Pay per Call /
Pay per Minute**

net900 ist konzipiert für die Bezahlung von digitalen Gütern, wie zum Beispiel Informationen, Musik, Spiele oder digitale Postkarten, die im Weiteren als kostenpflichtige Inhalte bezeichnet werden. Hierbei bietet net900 zwei Abrechnungsvarianten an: Bei 'Pay per Call'²⁵ zahlt der Kunde für die abgerufenen Inhalte einen einmaligen Betrag, z.B. 1,- DM für einen Zeitungsartikel. Bei 'Pay per Minute' werden die Inhalte zeitabhängig im Minuten-Takt abgerechnet, beispielsweise 1,- DM pro Minute für eine Online-Schachpartie.

Für die Abrechnung wird ein sogenanntes Inkassoverfahren verwendet, bei dem die Zahlungsbeträge für einen Kunden über einen bestimmten Zeitraum hinweg gesammelt und dann erst abgerechnet werden. Mit der Aufsummierung von Beträgen wird insbesondere eine wirtschaftliche Abrechnung von Kleinstbeträgen ermöglicht. In der klassischen Ausführung, bei net900 Classic, erfolgt die Abrechnung der kostenpflichtigen Inhalten über die Telefonrechnung. Hierbei werden die Gebühren in Telefoneinheiten umgerechnet, die dann über die Telefonrechnung des Kunden in einer aufaddierten Summe (also anonym) eingezogen werden. Die neuere Variante net900 Kontopass (seit Dezember 2000) ermöglicht die Abrechnung über das Girokonto des Kunden.

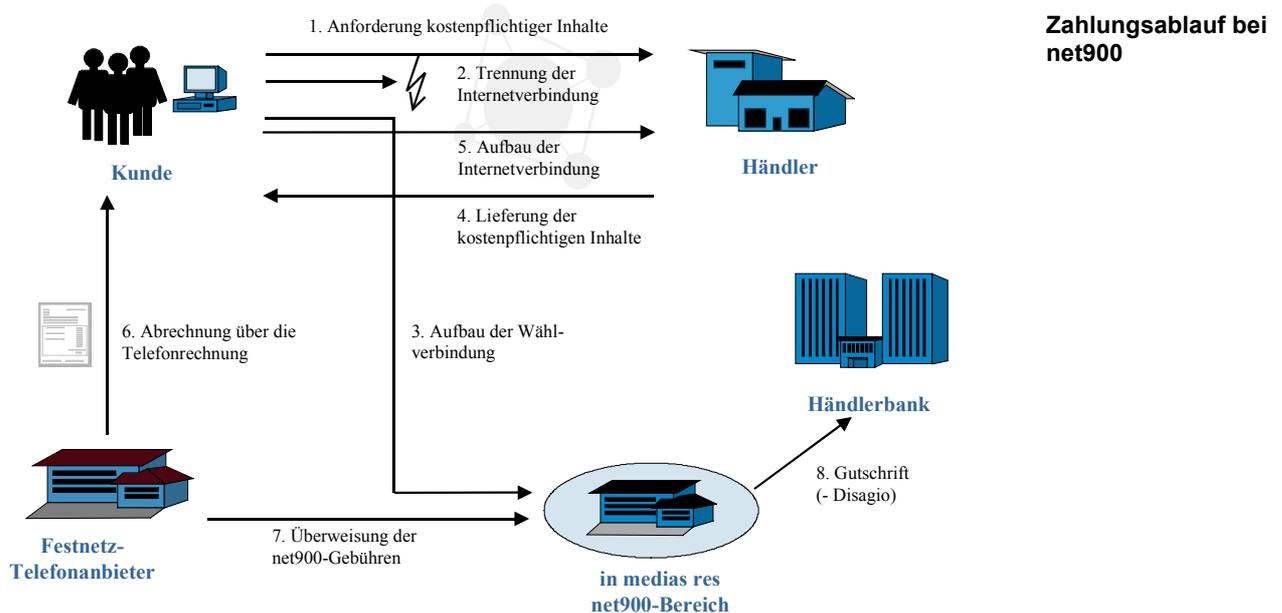
**Teilnehmer bei
net900**

Bei net900 Classic gibt es folgende Teilnehmer:

- den Kunden, der mit net900 kostenpflichtige Inhalte im Internet abrufen,
- den Händler, der net900 als Zahlungssystem in seinem Internet-Shop anbietet,
- die Firma 'in medias res', welche die net900-Zahlungen abwickelt,
- den Festnetz-Telefonanbieter, z.B. die Deutsche Telekom, der die Gebühren für die kostenpflichtigen Inhalte auf der Telefonrechnung des Kunden verbucht.

Eine Zahlung mit net900 Classic verläuft wie folgt:

²⁵ 'Pay per Call' ist die bei net900 verwendete Terminologie, die dasselbe wie das üblichere 'Pay per Click' bezeichnet. Die Bezeichnung 'Pay per Call' ist dadurch motiviert, dass durch den 'Click' kurzzeitig eine neue Verbindung (Call) aufgebaut wird (siehe Beschreibung des Zahlungsablaufs).



Zahlungsablauf bei net900

1. Anforderung kostenpflichtiger net900-Inhalte

Der Kunde möchte einen kostenpflichtigen Inhalt aus dem Internet-Shop des Händlers beziehen und wählt hierzu als Zahlungssystem net900 aus.

2. Trennung der Internetverbindung

Nachdem der Kunde sich mit der Übernahme der Kosten für die von ihm ausgewählten Inhalte einverstanden erklärt hat, wird die bestehende Internet-Verbindung getrennt. Dies wird durch eine beim Kunden zuvor installierte net900-Software realisiert.

3. Aufbau der Wahlverbindung

Anschließend wird automatisch eine Wahlverbindung zum net900-Bereich der Firma „in medias res“ aufgebaut. Im net900-Bereich sind die kostenpflichtigen Inhalte des Händlers abgelegt oder es wird von dort aus auf diese Inhalte verwiesen.

4. Lieferung der kostenpflichtigen Inhalte

Dem Kunden werden die von ihm angeforderten kostenpflichtigen Inhalte zugänglich gemacht. Das bedeutet beispielsweise, dass er den gewünschten Zeitungsartikel aus dem Zeitungsarchiv beziehen oder mit der Online-Schachpartie beginnen kann.

5. Aufbau der Internet-Verbindung

Nachdem der Kunde den kostenpflichtigen Inhalt bezogen hat, wird die Wählverbindung getrennt und die Internetverbindung wiederhergestellt.

6. Abrechnung über die Telefonrechnung

Die Gebühren für die Nutzung der kostenpflichtigen Inhalte werden dem Kunden über die Telefonrechnung des Festnetz-Telefonanbieters in Rechnung gestellt.

7. Überweisung der net900-Gebühren

Der Festnetz-Telefonanbieter überweist die auf der Telefonrechnung ausgewiesenen net900-Gebühren an 'in medias res'.

8. Gutschrift

Der Händler erhält von „in medias res“ unter Abzug eines Disagios die aufaddierten Gebühren für seine kostenpflichtigen Inhalte.

Voraussetzungen

**Voraussetzungen
des Kunden**

Damit der *Kunde* mit net900 zahlen kann, muss er zuvor folgende Voraussetzungen erfüllen:

- net900-Software

Der Kunde muss auf seinem Rechner die net900-Software²⁶ installieren, die als ein zusätzliches Modul (Plug-In) für den Internet-Browser ausgelegt ist. Die Internet-Kommunikation wird fortan von der Software mit verfolgt. Ruft der Kunde einen kostenpflichtigen net900-Inhalt auf, wird der Wechsel in den net900-Bereich durchgeführt.

- Anbindung

Damit während des Zahlungsablaufs eine Wählverbindung aufgebaut werden kann, ist es notwendig, dass der Internetzugang über ein Modem oder eine ISDN-Karte erfolgt. ADSL (T-DSL) oder eine Verbindung ins Internet aus einem Unternehmens-Netzwerk heraus wird zur Zeit nicht unterstützt. Außerdem darf der Telefonanschluss nicht für kostenpflichtige Anrufe gesperrt sein, da der Aufbau der Wählverbindung über eine 0192-Nummer funktioniert.

²⁶ Die net900-Software ist nur für Microsoft Windows-Systeme verfügbar und wird unter <http://www.net900.de> kostenlos zur Verfügung gestellt.

Voraussetzungen für den *Händler*, um net900 als Zahlungssystem in seinem Internet-Shop anbieten zu können:

**Voraussetzungen
für den Händler**

- Händler-Vertrag

Der Händler muss mit einem Kooperationspartner von net900 einen Vertrag schließen, in dem die Abrechnungsvarianten und die einzelnen Tarife vereinbart werden.

(a) Abrechnungsvarianten

Der Händler kann die beiden Abrechnungsvarianten „Pay per Call“ und „Pay per Minute“ wählen.

(b) Tarife

Über die Tarife legt der Händler fest, welche Gebühren der Kunde für den Abruf kostenpflichtiger Inhalten zu zahlen hat. Als Tarife sind entweder 0,29 bis 4,99 DM bei „Pay per Minute“ oder 0,29 bis 25 DM bei „Pay per Call“ möglich und sind den net900-Preislisten zu entnehmen.

Nach Abschluss des Vertrages erhält der Händler von „in medias res“ für die gebuchten Tarife die zugehörigen Tarifkennungen, die den jeweiligen kostenpflichtigen Inhalten hinzugefügt werden.

Der Vertrag gilt für die Dauer von einem Jahr. Die Kündigung muss drei Monate vor Ablauf eines Jahres erfolgen, ansonsten verlängert sich der Vertrag um ein weiteres Jahr.

- Anpassen der Internet-Seiten

Der Händler muss die Verweise (Links) zu den kostenpflichtigen Inhalten anpassen, indem er sie als net900-Links kenntlich macht und ihnen die vorgesehene Tarifkennung zuweist. Beispielsweise könnte der Verweis www.kinderkrebsstiftung.de in der net900-Syntax wie folgt aussehen: `www.kinderkrebsstiftung.de/net900?spende5DM.html,tarif=10121`.

Anhand solcher Verweise erkennt die net900-Software des Kunden, dass es sich um einen kostenpflichtigen net900-Inhalt handelt, der mit der angefügten Tarifkennung zu verrechnen ist.

- Ablage des kostenpflichtigen Inhalts

Der Händler muss die kostenpflichtigen Inhalte in den net900- Bereich der Firma „in medias res“ ablegen bzw. es muss vom net900-Bereich aus auf diese Inhalte verwiesen werden. Dazu sind drei Möglichkeiten vorgesehen:

- Der Händler legt seine kostenpflichtigen Inhalte auf dem bereitgestellten net900-Server ab (Webhosting). Diese Möglichkeit besteht nur für stati-

**Spezielle Ablage
der kostenpflichti-
gen Inhalte**

sche Daten. Dynamische Inhalte, beispielsweise Daten, die aus einer Datenbank generiert werden, lassen sich über diese Variante nicht ablegen.

- Der Händler mietet einen Stellplatz im net900-Bereich und stellt dort einen eigenen Server mit seinen kostenpflichtigen Inhalte auf (Webhousing).
- Der Händler legt seine kostenpflichtigen Inhalte auf seinem eigenen Server ab und schaltet eine Standleitung zum net900-Bereich (Virtual Private Network). Wählt ein Kunde sich in den net900-Bereich ein, um die Inhalte des Händlers abzurufen, wird dieser zum Händler-Bereich weiter geleitet²⁷.

Kosten

Dem Kunden entstehen bei der Nutzung von net900 keine zusätzlichen Kosten.

Die folgende Aufstellung der Händlerkosten für net900 Classic sind den Vertragsunterlagen der isoft GmbH²⁸, (Stand 01.06.2000) entnommen.

Kosten für den Händler

Einrichtungsgebühr	75,- DM
Monatliche Grundgebühr	7,50 DM
Gebühr pro Transaktion	je nach gebuchtem Tarif zwischen 15-35% ²⁹
Monatliche Gebühren bei Ablage der kostenpflichtigen Inhalten auf dem net900-Server pro MB (ab 50 MB)	0,12 DM
Monatliche Gebühren bei Abstellen eines Servers im net900-Bereich	85,- DM
Einmalige Gebühr bei Anbindung einer Standleitung	300,- DM
Monatliche Gebühr bei Anbindung einer Standleitung	85,- DM

²⁷ Dabei handelt es sich um eine sehr aufwändige Infrastruktur, da die Datenübertragung zum Händler über ein VPN (Virtual Privat Network) gesichert sein muss.

²⁸ Anbieter des net900-Systems

²⁹ Die hohen Transaktionsgebühren entstehen durch die Inkassodienstleistung bzw. den 0192-Dienst des Festnetz-Telefonanbieters.

2.6 eCash

eCash ist ein softwarebasiertes Zahlungssystem, bei dem der Kunde von seinem Girokonto digitale Münzen in eine elektronische Geldbörse auf seinem PC lädt. Mit den Münzen kann er in Internet-Shops, die eCash akzeptieren, einkaufen. Der Händler reicht die vom Kunden erhaltenen digitalen Münzen bei der Bank elektronisch ein, worauf ihm der Betrag auf einem konventionellen Konto gutgeschrieben wird. In einem Pilotprojekt (Start: Oktober 1997) wurde das eCash-System von der Deutschen Bank getestet. Am 25. Mai 2001 stellte sie eCash wegen mangelnder Kundennachfrage ein.

Hinter eCash steht die Idee, für das Internet ein Zahlungssystem mit digitalen Münzen anzubieten, das alle guten Eigenschaften des üblichen Bargeldes besitzt und zudem sicher ist. Aus Kundensicht funktioniert das Bezahlen mit eCash ähnlich wie das Bezahlen mit Bargeld:

**Grundkonzept:
Digitales Bargeld**

Der Kunde transferiert von seinem Konto digitale Münzen in seine elektronische Geldbörse (Abheben von Bargeld). Beim Kauf sendet er dem Händler den entsprechenden Betrag an digitalen Münzen (Bezahlen mit Bargeld). Der Händler reicht die Münzen bei seiner Bank ein und erhält den Betrag auf seinem Konto gutgeschrieben (Einzahlen von Bargeld). Bei eCash können die digitalen Münzen keinem bestimmten Kunden zugeordnet werden, wodurch der Kunde – wie beim Bezahlen mit Bargeld - gegenüber der Bank und dem Händler hinsichtlich der Zahlung vollständig anonym bleibt.

Das Besondere bei eCash ist, dass der Kunde (und nur der Kunde), für den Fall, dass der Händler den Erhalt einer Zahlung abstreitet, seine Anonymität aufheben kann³⁰.

**Aufhebung der
Anonymität**

Bei eCash gibt es folgende Teilnehmer:

Teilnehmer

- den Kunden, welcher mit eCash-Münzen seine Zahlung tätigt,
- den Händler, der eCash als Zahlungssystem in seinem Internet-Shop anbietet,
- die eCash-Bank, die digitale Münzen ausgibt, die vom Händler eingereichten Münzen überprüft und den Tausch von realem Geld in eCash-Münzen (und umgekehrt) sicherstellt.

**Laden der Geld-
börse**

³⁰ Jede Zahlung erzeugt ihre eigene Quittung in einer verschlüsselten Form, die nur der Kunde entschlüsseln kann, um zu beweisen, dass eine bestimmte Zahlung stattgefunden hat.

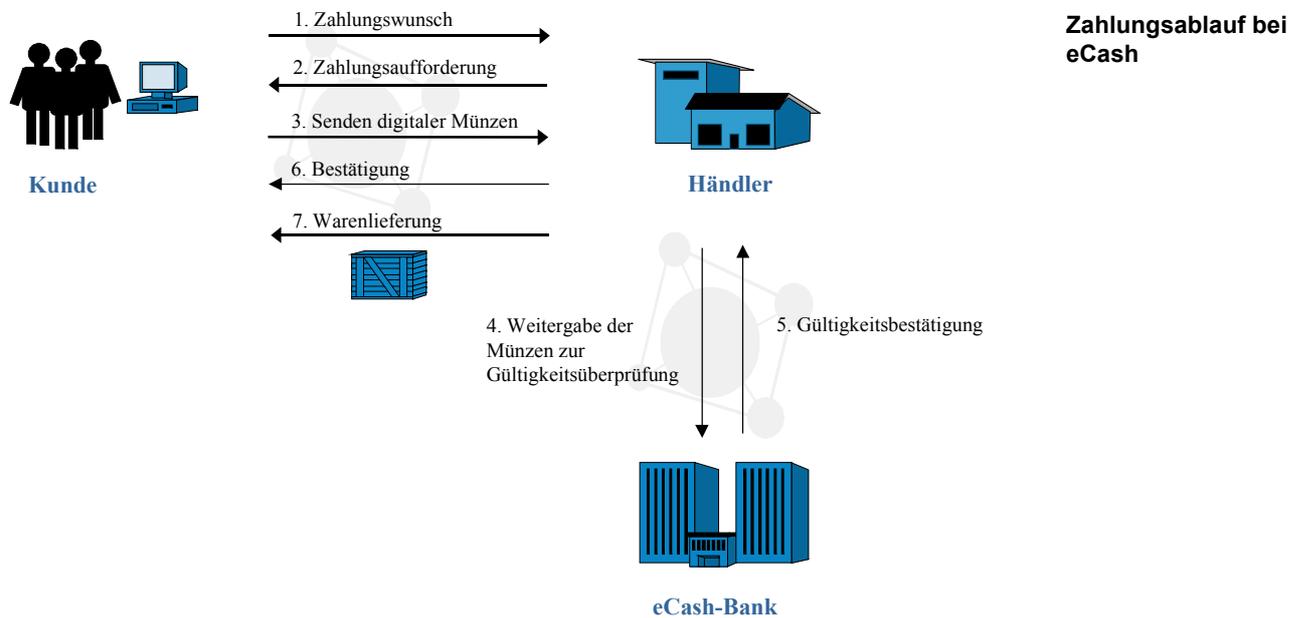
Vor dem Einkauf muss der Kunde zunächst seine auf dem PC installierte elektronische Geldbörse mit digitalen Münzen laden, was in folgenden Schritten abläuft:

- Schritt 1: Der Kunde eröffnet ein eCash-Konto und überweist auf dieses Konto mit einem konventionellen Überweisungsauftrag den von ihm gewünschten Betrag.
- Schritt 2: Der Kunde erzeugt auf seinem PC einen Münzrohling mit dem von ihm gewünschten Geldbetrag und versieht den Rohling mit einer fälschungssicheren Seriennummer (ähnlich der Seriennummer auf einem Geldschein), welche die Münze eindeutig identifiziert.
- Schritt 3: Die Seriennummer wird durch ein Verfahren verschlüsselt, das sich „blinding“ nennt. Die Seriennummer ist zwar noch vorhanden, für einen Dritten aber nicht lesbar (bildlich gesprochen "in einem Briefumschlag"). Die so veränderte Münze wird zum Signieren an die Bank geschickt.
- Schritt 4: Die Bank signiert die Münze des Kunden mit einem Gültigkeitsstempel³¹, ohne auf die Seriennummer zugreifen zu können (bildlich: "der Gültigkeitsstempel der Bank geht durch den Briefumschlag"), und sendet die so gültig gemachte Münze dem Kunden verschlüsselt zu.
- Schritt 5: Der Betrag der eCash-Münze wird vom Girokonto eingezogen.
- Schritt 6: Die elektronische Geldbörse entschleierte (entschlüsselt) die Seriennummer, ohne das Gültigkeitssiegel zu verletzen (unblinding) und speichert die Münze ab. Die Münze kann nun zum Bezahlen verwendet werden.

Nach dem Laden der Geldbörse besitzt der Kunde gültige, zum Bezahlen verfügbare Münzen, ohne dass die Bank die Seriennummer kennt. Digitalen Münzen können vom Kunden aber auch wieder auf das Konto eingezahlt werden (Entladen der Geldbörse).

Der Zahlungsvorgang mit eCash läuft wie folgt ab:

³¹ Bei dem Gültigkeitsstempel handelt es sich um die digitale Signatur der Bank.



Zahlungsablauf bei eCash

1. Zahlungswunsch

Der Kunde wählt im Online-Angebot des Händlers das Zahlungssystem eCash aus, um seine Zahlung zu tätigen.

2. Zahlungsaufforderung

Der Händler sendet dem Kunden eine Zahlungsaufforderung.

3. Senden digitaler Münzen

Stimmt der Kunde der Zahlungsaufforderung zu, so sendet er dem Händler den entsprechenden Betrag in digitalen Münzen zu.

4. Weitergabe der Münzen zur Gültigkeitsüberprüfung

Der Händler leitet die Münzen an die eCash-Bank weiter. Diese prüft, ob die Münzen schon einmal bei der Bank eingereicht wurden³² und ob es sich um eine von der Bank in Umlauf gebrachte Münze handelt³³. Wenn die Überprü-

³² Die Seriennummer jeder bei der eCash-Bank eingereichten Münze wird in einer Datenbank vermerkt. Der Versuch, eine Münze mehrmals einzulösen, wird nach einer Datenbank-Überprüfung (Double Spending-Check) erkannt und von der Bank zurückgewiesen. Das Verfahren stellt sicher, dass jede Münze nur einmal zur Zahlung verwendet werden kann.

³³ Hier wird die Echtheit des Gültigkeitsstempels (also der digitalen Unterschrift der Bank) auf den Münzen geprüft wird.

fung erfolgreich verlaufen ist, wird der Betrag dem eCash-Konto des Händlers gutgeschrieben.

5. Gültigkeitsbestätigung

Die Bank bestätigt dem Händler die Gültigkeit der digitalen Münzen.

6. Bestätigung

Der Kunde erhält eine Bestätigung, dass die Zahlung erfolgreich verlaufen ist.

7. Warenlieferung

Der Händler kann nun die Warenauslieferung in die Wege leiten.

Die Beträge auf dem eCash-Konto kann der Händler jederzeit seinem Girokonto gutschreiben lassen.

Voraussetzungen

**Voraussetzungen
für den Kunden**

Damit der *Kunde* mit eCash zahlen kann, muss er zuvor folgende Voraussetzungen erfüllen:

- eCash-Konto
Der Kunde muss sich bei einer eCash-Bank anmelden und dort ein eCash-Konto eröffnen.
- eCash-Wallet
Der Kunde benötigt eine spezielle Software, die eCash-Wallet-Software, die die elektronische Geldbörse auf dem Rechner des Kunden realisiert. Diese Geldbörse erlaubt es dem Benutzer, elektronisches Bargeld von seinem Girokonto abzuheben oder dieses darauf einzuzahlen. Sie bewahrt die Münzen auf dem Rechner des Kunden auf und visualisiert dem Kunden beim Internet-Einkauf den Bezahlvorgang mit digitalen Münzen. Die eCash-Wallet kann bis maximal 400,- DM aufgeladen werden.

**Voraussetzungen
für den Händler**

Voraussetzungen für den *Händler*, um in seinem Internet-Shop eCash als Zahlungssystem anzubieten:

- eCash-Konto
Der Händler benötigt ein eCash-Konto bei einer eCash-Bank.

- eCash-Händler-Software

Der Händler muss auf seinem Server die eCash-Händler-Software installieren. Diese realisiert die Kommunikation mit der eCash-Wallet des Kunden, der eCash-Bank und stellt sogenannte Skripte (Hilfsprogramme) für die Kopplung des Zahlungssystems mit dem Internet-Shop zur Verfügung.

eCash ist ein von der Sicherheitskonzeption sehr ausgereiftes Zahlungssystem, das auf die Anforderungen des Mediums Internet hin optimiert wurde. Daraus erklären sich auch einige Faktoren, die für das Scheitern des eCash-Piloten angeführt werden:

Bewertung

- Kunden bevorzugen auch im Internet Zahlungsweisen, die von einem konventionellen Zahlungsverfahren abgeleitet sind.
- Bei eCash handelt es sich um ein Prepaid-System, bei dem der Kunde mit dem Laden der Geldbörse in Vorleistung tritt.
- Die Technik empfanden viele Kunden als nicht ausgereift und in der Handhabung zu kompliziert.
- Die Einstiegshürde um eCash nutzen zu können war zu hoch, da sowohl der Kunde als auch der Händler ein Konto bei einer eCash-Bank (im Falle für Deutschland bei der Deutschen Bank) eröffnen mussten.
- Viele Kunden hatten kein Vertrauen in die Realisierung der digitalen Geldbörse als reine Softwarelösung (Was passiert bei einem Systemcrash? Was bei einem Hackerangriff?)

3 Auswahl und Einsatz von Internet-Zahlungssystemen

Ein guter Web-Shop ist mehr als ein Schaufenster, über das der Händler dem Kunden seine Produkte präsentiert. Idealerweise soll er eine durchgängige Abwicklung von Geschäftstransaktionen in allen Phasen unterstützen. Entscheidend für die Kundenakzeptanz und den Aufbau einer Kundenbindung wird sein, inwieweit über das Medium Internet ein Vertrauensverhältnis zwischen Kunde und Händler aufgebaut werden kann. Der Auswahl der verwendeten Internet-Zahlungssysteme und der Gestaltung des Bezahlvorganges kommen hier eine Schlüsselfunktion zu.

3.1 Strukturierter Planungsprozess

Es empfiehlt sich, der Integration von Bezahlverfahren in eine Web-Site eine strukturierte Planung voranzustellen. Diese kann in folgenden Schritten erfolgen:

1. Auswahl der Bezahlverfahren und Bezahlssysteme, die in den Web-Shop integriert werden sollen. Erstellung eines Anforderungsprofils für die Zahlungslösung und Kostenanalyse der einzelnen Verfahren.

Anforderungsprofil

Ergebnis: Liste der zu integrierenden Bezahlverfahren.

2. Festlegung, inwieweit bei der Durchführung der Integration Dienste von Payment-Service-Providern in Anspruch genommen werden sollen, sowie Auswahl der entsprechenden Dienstleister.

Outsourcing-Konzept

Ergebnis: Liste der Outsourcing-Partner und deren Aufgaben.

3. Planung der Integration der Bezahlverfahren in das Online-Business. Dieser Schritt umfasst Aspekte, die über das Bezahlssystem an sich hinausgehen, wie z.B. die Umgestaltung der bestehenden Web-Site, Änderungen der internen Unternehmensorganisation (Abläufe, Verantwortlichkeiten), Schulung von Mitarbeitern.

Integrationsplanung

Ergebnis: Projektplan mit allen technischen und organisatorischen Maßnahmen und Aufgaben.

Auf die einzelnen Planungsphasen werden wir im Folgenden eingehen.

3.2 Auswahl der Internet-Zahlungssysteme

Die Auswahl der auf einer Web-Präsenz angebotenen Bezahlverfahren hängt stark von den Anforderungen des jeweiligen Online-Geschäfts ab. Daher empfiehlt es sich als ersten Schritt, ein Anforderungsprofil für die angestrebte Zahlungslösung zu erstellen. Der nachfolgende Anforderungskatalog kann Ihnen hierfür als Grundlage dienen.

Vielfältige Anforderungen an die Bezahlung im Internet

- **Anonymität**

Der Kunde kann den Wunsch haben, Produkte oder Dienstleistungen im Internet zu kaufen, ohne dabei seine Identität preisgeben zu müssen. Der Wunsch des Kunden kann darin begründet sein, seine Privatsphäre zu schützen, nicht mit ungewollter Werbung belästigt zu werden oder die Aufzeichnung eines Profils über sein Kaufverhalten zu verhindern. Für den Händler ist die Wahrung der Anonymität des Kunden durch das Zahlungssystem vor allem dann wichtig, wenn aus der Art seiner Produkte oder Dienstleistungen heraus Diskretion notwendig ist.

Die Anonymität der Bezahlung wird von Internet-Zahlungssystemen hierbei in unterschiedlichem Maße unterstützt. Einige Zahlungssysteme (wie z.B. eCash) unterstützen eine vollständige Anonymität des Kunden allen Teilnehmern des Zahlungssystems gegenüber. Darüber hinaus gibt es Zahlungssysteme (wie z.B. paybox oder SET), bei denen der Kunde einigen Teilnehmern des Zahlungssystems gegenüber anonym bleibt, anderen Teilnehmern gegenüber wiederum nicht.

- **Authentizität**

Ein Zahlungssystem soll sicherstellen, dass die an der Zahlungstransaktion beteiligten Partner (Kunde, Händler, Bank, Vermittler) auch diejenigen sind, für die sie sich ausgeben. Darüber hinaus soll die Integrität und die Gültigkeit einer Zahlungstransaktion gewährleistet sein, so dass z.B. ein vereinbarter Zahlungsbetrag nicht vom Kunden oder Händler im nachhinein verändert werden kann.

- **Vertraulichkeit**

Das Zahlungssystem soll ausreichenden Schutz vor Angriffen aus dem Internet bieten und Missbrauch möglichst weitgehend ausschließen. Über Verschlüsselungstechniken sollte sichergestellt werden, dass die Zahlungsdaten (z.B. Kreditkartennummern) nicht von unbefugten Dritten gelesen bzw. manipuliert werden können. Wichtig ist hierbei, dass auf jeder Übertragungstrecke im Zahlungsablauf die Zahlungsdaten ver-

schlüsselt werden. So erfolgt z.B. bei der Kreditkarte mit WebPOS die Übertragung der Kreditkartendaten vom Kunden zum Händler unverschlüsselt, wenn keine weiteren Maßnahmen getroffen werden. Für die Verschlüsselung muss der Händler selbständig sorgen.

- **Zahlungssicherheit**

Das Zahlungssystem soll gewährleisten, dass eine einmal vorgenommene Zahlung vom Kunden nicht abgestritten und nicht ohne weiteres rückgängig gemacht werden kann. Die Nicht-Abstreitbarkeit von Zahlungen gibt dem Händler die Sicherheit, dass eine im Internet abgewickelte Zahlungstransaktion auch zur tatsächlichen Gutschrift auf seinem Konto führt. Leider ist die Nicht-Abstreitbarkeit in einigen Internet-Zahlungssystemen, wie z.B. bei der Kreditkarte (ausgenommen bei SET) nicht umgesetzt. Hier besteht die Möglichkeit, dass ein Kunde bestreitet, eine im Internet vorgenommene Zahlung mit der Kreditkarte getätigt zu haben. In diesem Fall wird der Zahlungsbetrag dem Kunden unverzüglich gutgeschrieben und beim Händler wieder eingezogen. Die dadurch verursachte Zahlungsunsicherheit kann für den Händler monatelang nach der Zahlungsabwicklung im Internet (und womöglich nach der Auslieferung der Ware) bestehen.

- **Zeitpunkt der Gutschrift**

Die Gutschrift des Zahlungsbetrags auf dem Konto des Händlers soll schnellstmöglich oder zumindest zeitnah mit der Auslieferung der Ware an den Kunden erfolgen, so dass der Händler nicht in Vorleistung zu treten braucht. Für den Händler minimiert sich damit das Risiko, Waren bereits geliefert zu haben und der Zahlung „hinterherzulaufen“. Dies spielt vor allem bei digitalen Gütern eine große Rolle, denn hier ist der Nachweis, dass die Ware ausgeliefert wurde, nicht einfach zu führen (Beispiel: Herunterladen von Musik). Wenn es sich dann noch um Kleinstbeträge handelt, ist der Aufwand, die Zahlung einzufordern, häufig nicht mehr wirtschaftlich. Auf der sicheren Seite ist der Händler bei den sogenannten vorausbezahlten (prepaid) Zahlungssystemen, wie z.B. der Geldkarte.

Die Gutschrift des Zahlungsbetrages auf das Konto des Händlers ist auch betriebswirtschaftlich von Interesse. In der Regel gelangen die beim Kunden eingezogenen Beträge mit Verzögerung auf das Konto des Händlers. Die „Parkzeit“ der Beträge bei den Teilnehmern, die die Transaktionen für das jeweilige Zahlungssystem abwickeln, sind hier zu beachten. Beispielsweise werden bei paybox die Zahlungsbeträge beim

Kunden per Lastschriftverfahren eingezogen, gelangen aber im „worst case“ erst zwei Wochen später auf das Konto des Händlers.

- **Schutz vor Zahlungsausfällen**

Zusammen mit dem Zahlungssystem können Services angeboten werden, die das Risiko von Zahlungsausfällen für den Händler minimieren. Beispiele hierfür sind: Bonitätsprüfungen, Zahlungsabsicherungen oder Insolvenzübernahmen.

- **Transaktionsbearbeitung**

Über das Zahlungssystem sollen die Transaktionen möglichst automatisiert und bequem, ohne Aufwand für den Händler, abgewickelt werden können. Nach einer im Internet stattgefundenen Zahlung erfolgt für den Normalfall eine automatische Gutschrift des Zahlungsbetrags auf das Konto des Händlers sowie eine Abbuchung vom Konto des Kunden. Das System soll dem Händler aber auch die Möglichkeit bieten, über eine Schnittstelle einzelne Transaktionen nachzubearbeiten. Hierzu gehören beispielsweise die Festlegung oder Anpassung von Zahlungszielen, die Kopplung der Zahlungsabbuchung an den Liefertermin, Stornierungen und Gutschriften von Zahlungen.

Je automatisierter die Transaktionsbearbeitung eingesetzt werden kann, desto geringer die internen Verwaltungs- und Kommunikationskosten, die mit dem Einsatz des Zahlungssystems verbunden sind.

- **Nachvollziehbarkeit**

Jede über das Zahlungssystem stattgefundenene Transaktion soll aufgezeichnet und vom Händler online eingesehen werden können. Hierzu müssen für jede Transaktion alle wichtigen Informationen, wie zum Beispiel Datum, Uhrzeit und eine eindeutige Transaktionsnummer, festgehalten werden. Darüber hinaus soll es für den Händler möglich sein, eine wöchentliche oder monatliche Zahlungsaufstellung abzurufen.

- **Integration in die vorhandene Umgebung**

Das Zahlungssystem soll vorgefertigte Schnittstellen bereitstellen, die eine einfache Übernahme der Zahlungsdaten (z.B. Betrag, Transaktionsnummer) in andere beim Händler eingesetzte Programme, wie z.B. Auftragsbearbeitung oder Finanzbuchhaltung, erlauben. Viele Zahlungssysteme werden mit vorgefertigten Modulen für gängige Shop-Systeme, wie etwa Intershop, ausgeliefert, was die Integration in die vorhandene Umgebung erheblich erleichtert. Für die Zukunft wünschenswert wären

standardisierte Schnittstellen, die die Zahlungsdaten für alle Zahlungssysteme inhaltlich und formal eindeutig definieren.

Eine weitergehende Einpassung des Zahlungssystems in die beim Händler vorhandene Umgebung sollte über spezielle Programmierschnittstellen (sogenannte Application Programming Interfaces, APIs) möglich sein.

Insgesamt gilt: Je flexibler das Zahlungssystem in die vorhandene Umgebung eingepasst werden kann, desto höher ist der Automatisierungsgrad der Zahlungs- bzw. der E-Commerce-Prozesse und desto niedriger sind die damit verbundenen internen Verwaltungs- und Kommunikationskosten.

- **Services**

Für das Zahlungssystem sollen alle notwendigen Dienstleistungen zur Einrichtung und Anpassung in die beim Händler vorhandene Umgebung angeboten werden. Hierzu gehört auch ein Hotline-Service, den der Händler bei Fragen und Problemen - möglichst kostenfrei - in Anspruch nehmen kann.

- **Universalität**

Ein Bezahlverfahren soll in möglichst vielen Einkaufssituation die Bezahlung erlauben. Wünschenswert wäre hier ein Zahlungssystem, das sowohl im Internet als auch bei Einkäufen vor Ort eingesetzt werden kann. Beispiele hierfür sind die Geldkarte oder die Kreditkarte.

- **Internationalität**

Ein Internet-Zahlungssystem soll auch im Ausland von Kunden einfach genutzt werden können. Das klassische Beispiel hierzu ist die Kreditkarte, die weltweit als Zahlungssystem akzeptiert und verwendet wird. Für jedes andere Zahlungssystem sind die technischen und bankspezifischen Voraussetzungen im Einzelfall zu klären.

- **Zahlungsbetrag**

Mit dem Zahlungssystem sollen sich die in dem jeweiligen Online-Shop üblichen Zahlungsbeträge ökonomisch sinnvoll abwickeln lassen. So ist beispielsweise die Kreditkarte für die Bezahlung von Kleinstbeträgen (zum Beispiel 0,10 DM für das Herunterladen eines Zeitungsartikels) ungeeignet. Demgegenüber kann die Geldkarte nicht zur Bezahlung von hochpreisigen Waren über 400,- DM verwendet werden. Bei net900 wiederum kalkuliert der Händler die Preise für seine Waren nicht in erster

Linie nach ökonomischen Gesichtspunkten; die Festlegung richtet sich vielmehr nach den möglichen Zahlungsbeträgen, die net900 für den Händler vorgibt.

- **Voraussetzungen für Kunden**

Das Zahlungssystem soll von vielen Kunden genutzt werden können. Wichtig hierzu ist, dass die Nutzung eines Zahlungssystems mit möglichst wenigen Voraussetzungen verbunden ist, wie etwa das Abschließen eines Vertrages, Beschaffung von Hardware (Chipkartenleser) oder das Installieren einer speziellen Software.

- **Voraussetzungen für Händler**

Das Zahlungssystem soll für den Händler möglichst einfach einzusetzen sein und mit wenigen Voraussetzungen einhergehen. Die Einfachheit des Einsatzes sollte aber nicht auf Kosten der Integration des Zahlungssystems in den gesamten Geschäftsprozess bzw. in die vorhandene IT-Struktur gehen. Hier kann die Auslagerung von Aufwänden an Payment-Service-Provider erwogen werden (näheres im nächsten Abschnitt).

Eine Einordnung der in der Arbeit vorgestellten Internet-Zahlungssysteme in den Anforderungskatalog finden Sie in der folgenden Tabelle. Da die Entwicklung der einzelnen Zahlungssysteme am Markt sehr dynamisch verläuft und die jeweiligen Anforderungen stark von der Einsatzsituation abhängen, kann die Tabelle nur als erste, grobe Orientierung dienen, der eine detaillierte, auf den konkreten Fall bezogene Analyse folgen muss.

	paybox	net900	Lastschrift SSL	Kreditkarte SSL	Kreditkarte WebPOS	Kreditkarte SET	Geldkarte	eCash
Anonymität	●	●	○	○	○	●	●	●
Authentizität	●	●	○	○	○	●	●	●
Vertraulichkeit	●	●	●	●	●	●	●	●
Zahlungssicherheit	●	●	○	○	○	●	●	●
Zeitpunkt der Gutschrift	●	●	○	○	●	●	●	●
Schutz vor Zahlungsausfälle	●	●	○	○	●	●	●	●
Transaktionsbearbeitung	●	●	○	○	●	●	○	○
Nachvollziehbarkeit	●	●	●	●	●	●	●	●
Integration in die Umgebung	●	○	○	○	●	●	○	○
Services	●	●	○	○	●	●	●	●
Universalität	●	○	●	●	●	●	●	○
Internationalität	●	○	○	●	●	●	○	○
Zahlungsbetrag	●	●	●	●	●	●	●	●
Voraussetzungen für Kunden	●	●	●	●	●	●	●	○
Voraussetzungen für Händler	●	●	●	●	●	○	○	○

- Das Auswahlkriterium wird gut erfüllt.
- Das Auswahlkriterium wird ausreichend erfüllt.
- Das Auswahlkriterium wird weniger gut erfüllt.

Einordnung der Zahlungssysteme in den Anforderungskatalog

Ein wichtiger Punkt bei der Entscheidung für oder gegen ein Internet-Zahlungssystem sind die damit einhergehenden Kosten. Zusätzlich zu den Kosten, die dem Zahlungssystem direkt zugeordnet werden können, sind die innerbetrieblichen Kosten und Einsparungspotentiale zu betrachten, die vor allem die Integration in das technische und organisatorische Umfeld betreffen. Diese Kosten muss der Händler für seinen Internet-Shop individuell erfassen.

**Komplexe Kosten-
betrachtung**

3.3 Outsourcing von Teilaufgaben an Payment-Service-Provider

Nachdem feststeht, welche Zahlungsverfahren und Zahlungssysteme in Ihrem Internet-Shop eingesetzt werden sollen, stellt sich die Frage, wie diese

Zahlungssysteme, die auf oft recht komplexen Softwarelösungen basieren, technisch und organisatorisch in Ihre IT-Umgebung integriert und dann betrieben werden sollen.

Payment-Service-Provider

Bestehen hier Know-how- und personelle Engpässe, so bietet es sich an, externe Partner hinzuzuziehen, die sich auf Dienstleistungen im Umfeld von elektronischen Zahlungssystemen spezialisiert haben. Diese Dienstleister werden als Payment-Service-Provider bezeichnet. Payment-Service-Provider können ein sehr weites Spektrum von Dienstleistungen abdecken: dieses reicht von der technischen Integration eines Internetzahlungs-Systems in den Web-Shop, über die teilweise oder vollständige Abwicklung des elektronischen Zahlungsverkehrs für den Händler, bis hin zu weitergehenden Dienstleistungen, wie z.B. Vertragsabschluss, Inkassoverfahren und Integration der Zahlungsprozesse in die Unternehmensinfrastruktur.

Vielzahl von Realisierungsvarianten

Im Folgenden werden drei Realisierungsszenarien aufgeführt, die sich in ihrer Outsourcing-Tiefe unterscheiden:

- Szenario 1:
Die Zahlungssysteme werden von einem Payment-Service-Provider bereitgestellt. Die mit der Bezahlung einhergehenden Aufgaben, wie Integration in die IT-Umgebung, sicherheitstechnische Betreuung, Bonitätsprüfung der Kunden, Erstellen von Zahlungsstatistiken, Einleiten von Inkassoverfahren usw., werden weitgehend vom Payment-Service-Provider übernommen (Full-Service Payment-Lösung).
- Szenario 2:
Die Zahlungssysteme werden von einem Payment-Service-Provider lediglich bereitgestellt und systemtechnisch betreut. Die mit der Bezahlung einhergehenden Aufgaben, wie Integration in die IT-Umgebung, Bonitätsprüfung der Kunden, Erstellen von Zahlungsstatistiken, Einleiten von Inkassoverfahren usw., werden vom Händler eigenständig realisiert (gehostete Payment-Lösung).
- Szenario 3:
Der Händler integriert und betreibt ohne Outsourcing-Partner die Zahlungssysteme und die mit der Bezahlung einhergehenden Aufgaben.

Um Ihnen ein Gefühl für die entstehenden Aufwände zu vermitteln, soll im Folgenden die Vorgehensweise für Szenario 3 (Integration und Betreiben *eines* Zahlungssystems ohne Outsourcing-Partner) dargestellt werden:

- Sie beziehen das Zahlungssystem direkt bei dem Betreiber und schließen mit diesem die dazu notwendigen Verträge ab.
- Die Einbindung des Zahlungssystems in die Geschäftsprozesse werden von Ihnen geplant und organisatorisch vorbereitet.
- Das Zahlungssystem wird auf einen in Ihrem Unternehmen befindlichen Rechner installiert und konfiguriert, in den Internet-Shop eingebunden und in die vorhandene Systemumgebung integriert. Für die technische Anbindung an die vorhandene DV-Landschaft (etwa ERP-System) werden geeignete Schnittstellen spezifiziert und realisiert.
- Der Einsatz von Zahlungssystemen geht notwendigerweise mit einer aufwendigen Sicherheitsinfrastruktur einher, die Sie planen, implementieren und überwachen.
- Das Zahlungssystem wird in Ihrem Unternehmen im laufenden Betrieb technisch administriert und gewartet.
- Alle organisatorischen und verwaltungstechnischen Aufgaben rund um den Zahlungsverkehr (Freischalten von Abbuchungen, Auswertung der Zahlungsdaten, usw.) werden im vollen Umfang von Ihnen geleistet.

Die hohen technischen und organisatorischen Aufwände werden auch durch die Erfahrungen der Autoren bei der Integration einer Reihe von Internet-Zahlungsverfahren in das Online-Spendenmodul der Deutschen Kinderkrebsstiftung (www.kinderkrebsstiftung.de) bestätigt.

Halten Sie in Ihrem Unternehmen kein technisches Know-how vor, so empfiehlt es sich, möglichst viele Leistungen einem Payment-Service-Provider zu übertragen und sich auf die Auswahl der Bezahlverfahren und des Payment-Service-Providers zu konzentrieren.

Empfehlung

Mehrere Internet-Zahlungssysteme in einem Shop

Wollen Sie Ihren Kunden in Ihrem Shop-System mehrere Internet-Zahlungssysteme zur Auswahl anbieten, so vervielfältigen sich die technischen und administrativen Aufwände entsprechend: Bei der Integration eines weiteren Internet-Zahlungssystems ergeben sich zur Zeit kaum Synergieeffekte aus vorgehenden Integrationsprojekten. Dies hat folgende Gründe:

- Jedes Zahlungssystem ist technisch anders aufgebaut und besitzt eigene Schnittstellen zur Anbindung an das Shopsystem.
- Jedes Zahlungssystem besitzt eine spezifische Logik für das Management des Zahlungsverkehrs. Beispiel: Stornierung einer Zahlung.

Wünschenswert aus Sicht des Händlers wäre hier eine integrierte Gesamtlösung für die Internet-Bezahlung, die mehrere Internet-Zahlungssysteme um-

fasst und sich zudem technisch und organisatorisch einfach in eine E-Commerce-Lösung integrieren lässt.

Gegenwärtig bringen die verfügbaren Internet-Zahlungssysteme nur ansatzweise die hierzu notwendigen Voraussetzungen mit. Hinsichtlich dieses Integrationsaspektes könnten Payment-Service-Providern künftig eine Schlüsselrolle spielen, indem Sie dem Händler eine einheitliche Sicht auf Zahlungstransaktionen, Reports, Schnittstellen zu anderen Systemen oder Funktionen zum Erstellen von Gutschriften, unabhängig von den jeweiligen Zahlungssystemen, bieten.³⁴

3.4 Integration in das Online-Business - Checkliste

In diesem Abschnitt soll die Integration der Bezahlverfahren aus Kundensicht betrachtet werden. Sehen wir uns hierzu den Ablauf eines typischen Online-Einkaufes an.

Ängste und Vorbehalte des Kunden

Der Kunde informiert sich zunächst auf der Web-Site über die angebotenen Produkte; er stellt dann einen Warenkorb zusammen. Schließlich soll die Kauftransaktion über das Internet durchgeführt werden. An dieser Stelle entstehen beim Kunden oft Bedenken und Sorgen, da

- er persönliche Daten weitergeben muss,
- er nicht weiß, was mit diesen Daten passiert,
- diese Daten missbraucht werden könnten,
- er nicht sicher weiß, ob der Shop im Netz vertrauenswürdig ist,
- er nicht weiß, was er tun soll, wenn nicht geliefert wird oder wenn bei der Zahlungstransaktion ein Fehler auftritt.

Leider sind diese Vorbehalte nicht ganz unbegründet, wie Testeinkäufe der Stiftung Warentest gezeigt haben [TÖP00]. Ganz wesentlich für die Akzeptanz ist es daher, die Zahlungsabläufe in einer Web-Site so zu gestalten, dass beim Kunden Vertrauen aufgebaut wird.

Eine gute Orientierung geben hier die WebTrust-Standards, die die weltweit umfassendsten Prinzipien für vertrauenswürdige Transaktionen im Bereich des E-Commerce darstellen. Die WebTrust-Standards wurden vom American

³⁴ In einem Projekt an der Fachhochschule Bonn-Rhein-Sieg werden zur Zeit die Dienste von Payment-Service-Providern zusammengestellt und vergleichend analysiert.

Institute of Certified Public Accountants (AICPA) entwickelt und sind im Internet verfügbar [AICPA1] [AICPA2] [AICPA3] [AICPA4].

Entlang der Prinzipien dieser Standards wollen wir im folgenden Hinweise für eine kundenorientierte Integration von Bezahlverfahren in eine E-Commerce-Site geben. Die folgenden Checklisten gehen davon aus, dass Sie Internet-Zahlungssysteme in Ihrem Shop bereits einsetzen und diese auf Vertrauenswürdigkeit hin testen möchten.

3.4.1 Prinzip: Schutz persönlicher Daten

Für den Kunden ist es wichtig, darauf vertrauen zu können, dass seine persönlichen Daten durch wirksame Maßnahmen geschützt werden. Weiterhin möchte er die Souveränität über die von ihm gegebenen Informationen behalten und wissen, wohin seine Informationen fließen und für welche Zwecke sie benutzt werden.

Privatsphäre des Kunden achten

3.4.2 Checkliste 'Schutz persönlicher Daten'

- Informieren Sie den Kunden, wenn er es wünscht, über die Funktion des verwendeten Zahlungssystems?
- Informieren Sie den Kunden darüber, welche Daten Sie über ihn speichern (z.B. Lieferadresse, Kreditkartennummer, Kontonummer)?
- Informieren Sie den Kunden, warum Sie seine Daten brauchen und was Sie mit diesen Daten machen?
- Unterscheiden Sie in den Eingabemasken diejenigen Felder, die der Kunde ausfüllen muss, von denjenigen, die er ausfüllen kann?
- Ermöglichen Sie dem Kunden einen Zugriff auf seine von Ihnen gespeicherten Daten und geben Sie ihm eine Möglichkeit, die Daten, die nicht notwendigerweise (z.B. auf Grund der gesetzlichen Aufbewahrungspflicht) bei Ihnen gespeichert sein müssen, zu ändern und zu löschen?
- Informieren Sie den Kunden darüber, an wen Sie seine Daten weiterleiten?

- Versichern Sie sich, dass die von Ihnen in Anspruch genommenen Service-Provider (Internet-Service-Provider, Payment-Service-Provider) die Daten ebenso vertraulich behandeln wie Sie?
- Geben Sie dem Kunden eine möglichst weitgehende Kontrolle über die Verwendung seiner Daten (z.B. Verwendung der Adressdaten, um Werbeaktionen durchzuführen)?
- Stellen Sie durch entsprechende organisatorische und technische Maßnahmen sicher, dass die von Ihnen gegebenen Zusicherungen auch eingehalten werden?
- Informieren Sie den Kunden darüber, wenn Sie mit seinen Daten anders umgehen?
- Genügt der Umgang mit den Kunden- und Zahlungsdaten den Datenschutzbestimmungen?

3.4.3 Prinzip: Sicherheit

Während des Zahlungsablaufs findet zwischen den an der Transaktion Beteiligten ein komplexer Informationensaustausch über das Internet statt. Da es sich hier um sensible Informationen handelt, ist sicherzustellen, dass sie bei ihrem Weg über das Netz und bei der anschließenden Speicherung in den E-Commerce-Systemen der Beteiligten vor unberechtigtem Zugriff geschützt sind (empfehlenswerte Literatur zur Internetsicherheit: [LEP00] [RAE98]). Dies verlangt bei der Übertragung über das Internet den Einsatz von kryptografischen Verfahren (empfehlenswerte Literatur zur Kryptografie: [BEU99] [SEL00]) und die Absicherung der E-Commerce-Systeme durch Zugangskontrollmechanismen (im einfachsten Fall: Passwortschutz und Rechtevergabe).

Die Sicherheit eines Internet-Zahlungssystems darf keinesfalls isoliert betrachtet werden, sondern ist im Zusammenhang mit der gesamten System- und Netzumgebung zu sehen. Auch die Einbettung in das organisatorische Umfeld ist in die Betrachtung einzubeziehen. Diesem Aspekt wird in der nachfolgenden Checkliste Rechnung getragen.

Es zeigt sich, dass die Aufwände für ein angemessenes Sicherheitsniveau beträchtlich sind und nur von Unternehmen mit einem auf Sicherheit geschulten IT-Bereich im vollen Umfang zu leisten sind. Kleinere und mittlere Unternehmen werden oft überfordert sein. Dies spricht in vielen Fällen dafür,

**Sicherheit als
ganzheitliche
Fragestellung**

sicherheitsrelevante E-Commerce-Komponenten, insbesondere Internet-Zahlungssysteme, soweit wie möglich in die Verantwortung eines Outsourcing-Partners zu geben. Die folgende Checkliste kann dann bei der Auswahl des Outsourcing-Partners behilflich sein.

3.4.4 Checkliste 'Sicherheit'

- Existiert für Ihr E-Commerce-Geschäft eine Sicherheitskonzeption, aus der verbindliche Sicherheitsrichtlinien abgeleitet wurden?
- Sind in Ihrem Unternehmen organisatorische Maßnahmen für eine kontinuierliche Überwachung der Sicherheitsrichtlinien eingerichtet? Werden regelmäßige Audits zur Einhaltung der Richtlinien abgehalten?
- Wird das eingesetzte Personal regelmäßig im Bezug auf Sicherheit geschult?
- Ist in Ihrem Unternehmen eine Stelle eingerichtet, an die sich der Kunde bei einem Verdacht auf Sicherheitslücken wenden kann? Beispiel: Verdacht auf Missbrauch der Konten- oder Kreditkartendaten.
- Gibt es in Ihrem Unternehmen eine Person, die für die Konzeption und die Umsetzung der Sicherheitsrichtlinien verantwortlich ist?
- Ist durch entsprechende Vereinbarungen (Service-Level-Agreements) sichergestellt, dass auch Ihre Outsourcing-Partner die gleichen Sicherheitsstandards garantieren wie Sie?
- Ist für Ihre E-Commerce-Präsenz genau festgelegt, welche Personen auf welche Daten (z.B. Kreditkartendaten der Kunden) zugreifen dürfen?
- Existieren geeignete technische und organisatorische Maßnahmen, um die Zugriffsrichtlinien durchzusetzen und zu überwachen? Dies betrifft sowohl die Ebene der Betriebssysteme (Systemadministratoren) als auch die Ebene der Datenbanken (Datenbankadministratoren) und die der Applikationen (Endanwender).
- Sind auch auf der physischen Ebene Ihre E-Commerce-Systeme und insbesondere die Zone mit den Zahlungssystemen vor unbefugtem Zugriff geschützt (Einbruch, Zutritt zum Serverraum)?

- Sind Kontrollmechanismen implementiert, die mögliche Angriffe auf Ihr System erkennen und automatische Maßnahmen für einen solchen Fall einleiten (Intrusion-Detection-Systeme)?
- Sind standardisierte Vorgehensweisen sowohl für den Fall eines Sicherheitsangriffes auf logischer Ebene (Hacker) als auch eines allgemeinen Notfalls (z.B. Feuer, Stromausfall, Wasserschäden) definiert?
- Gibt es Verfahren für das Change-Management Ihrer E-Commerce-Umgebung? Beispiele: Test neuer Versionen des Zahlungssystems, Einspielen neuer Versionen im laufenden Betrieb.
- Sind die von Ihnen eingesetzten Technologien des aktiven Web-Contents (Java Applets, ActiveX, Skripte) auf Sicherheitslücken getestet? Beispiel: Internet-Zahlungssysteme sind oft über Skripte mit den Warenwirtschaftssystemen gekoppelt.
- Wird die eingesetzte Software routinemäßig auf Viren und trojanische Pferde getestet? Beispiel: Über ein trojanisches Pferd (=eingeschleuste Hackersoftware) könnte auf die Kreditkarten- oder Kontendaten Ihrer Kunden zugegriffen werden.
- Ist der Zugriff nicht berechtigter Personen auf Ihr internes Netz hinreichend geschützt? Beispiel: Abschottung des internen Netzes über einen Firewall, Sperrung nicht benötigter Netzdienste.
- Sind die zur Datensicherung abgelegten Datenträger vor unbefugtem Zugriff geschützt?
- Benutzen Sie für die Kommunikation möglichst weitgehend gesicherte SSL-Verbindungen?
- Hat das eingesetzte technische Personal das notwendige Know-how für die Einrichtung und das Management der gewünschten Sicherheitspolitik?

3.4.5 Prinzip: Verfügbarkeit

Abgeschlossene Zahlungs- transaktionen

Für einen Kunde im Internet ist es wichtig, dass er den gesamten Einkauf von der Informationsphase über die Zusammenstellung seines Warenkorbs bis hin zur rechtsverbindlichen Bestellung und Bezahlung als eine geschlossene Einheit ohne Unterbrechung oder Störung abwickeln kann. Daher kommt der

Verfügbarkeit des E-Commerce-Gesamtsystems (Internetzugang / Intranet / Datenbank / Webpräsenz / Zahlungssystem) eine entscheidende Bedeutung zu. Nichts kann einen Kunden so sehr verunsichern wie undefinierte Systemzustände im Umfeld eines Zahlungsvorgangs.

3.4.6 Checkliste 'Verfügbarkeit'

- Ist ein durchgehender Internetzugang zu Ihrer Site gewährleistet?
- Wird Ihr System (Server) kontinuierlich auf Verfügbarkeit hin überwacht?
- Kann Ihnen Ihr Internet-Service-Provider oder Payment-Service-Provider die notwendigen Verfügbarkeiten garantieren?
- Welche Maßnahmen existieren für Ausnahmesituationen (Fehlerfall, Überlastsituation)?
- Ist Ihr Personal für den Ausnahmefall entsprechend geschult?
- Werden Fehlbedienungen und unklare Systemzustände während des Zahlungsvorgangs abgefangen?
- Ist eine korrekte Abarbeitung der Zahlungstransaktionen nach einem Systemzusammenbruch gewährleistet? Stichwort: Doppelabbuchung.
- Kann der Kunde sicher feststellen, dass eine Zahlungstransaktion erfolgt ist?
- Kann der Kunde sicher sein, dass keine Zahlung ausgelöst wurde, wenn keine Bestätigung durch das System erfolgt ist?
- Kann der Kunde nach unklaren Systemzuständen den Status der Zahlungstransaktion in Erfahrung bringen, um festzustellen, ob er den Zahlungsvorgang nochmals durchführen muss?

3.4.7 Prinzip: vereinbarungsgemäße Geschäftsabwicklung

Das Prinzip der vereinbarungsgemäßen Geschäftsabwicklung beruht darauf, dass Sie Ihren Kunden in Form einer Selbstverpflichtungserklärung (disclosure) offen legen, wie Sie Ihr E-Commerce-Geschäft betreiben. Diese Erklä-

Selbstverpflichtungserklärung

rung muss geeignet sein, beim Kunden das Vertrauen zu bestärken, dass Sie Ihren Verpflichtungen nachkommen möchten und dazu auch technisch und organisatorisch im Stande sind. Wird dies von neutraler Seite überprüft und besiegelt, so stärkt das zusätzlich Ihre Vertrauensstellung.

Die Umsetzung dieses Prinzips kann in folgenden Stufen erfolgen.

- Schritt 1:
Sie legen die vertrauensbildenden Maßnahmen fest, die Sie dem Kunden zusichern möchten.
- Schritt 2:
Sie richten Verfahrensweisen ein, die geeignet sind, die Einhaltung der vertrauensbildenden Maßnahmen sicherzustellen. Diese Verfahrensweisen werden von Ihnen dokumentiert.
- Schritt 3:
Sie machen dem Kunden Ihre vertrauensbildenden Maßnahmen über Ihre Web-Präsenz transparent.

Für die Umsetzung der Schritte 1 und 2 können Sie die Checklisten aus den vorangehenden Abschnitten verwenden.

Selbstauskunft

Wählen Sie aus den Checklisten diejenigen Punkte aus, die Sie Ihren Kunden zusichern möchten, und geben Sie – in Form einer Selbstauskunft – Ihre technischen und organisatorischen Maßnahmen hierzu explizit an.

Beispiele:

Checkpunkt:

"Ermöglichen Sie dem Kunden einen Zugriff auf seine von Ihnen gespeicherten Daten und geben Sie ihm eine Möglichkeit, diese zu ändern und auch zu löschen?"

Maßnahmen:

Registrierte Kunden erhalten einen (passwortgeschützten) Zugriff auf ihr Benutzerprofil, in dem sämtliche über sie gespeicherten Daten enthalten sind. Alle Daten (mit Ausnahme des Nachnamens und der Kundennummer) können vom Kunden geändert werden. Falls keine aktuelle Transaktion läuft, hat der Kunde die Möglichkeit, seine über ihn gespeicherten Daten aus der Datei zu löschen. Für eventuelle Rückfragen oder Namensänderungswünsche stehen dem Kunden zusätzlich ein E-Mailkontakt und eine Telefonnummer zur Verfügung.

Checkpoint:

"Informieren Sie den Kunden, wenn er es wünscht, über die Funktion des verwendeten Zahlungssystems?"

Maßnahmen:

Zu jeder der dem Kunden angebotenen Zahlungsalternativen existiert ein Informations-Button, der auf eine erklärende Seite des Zahlungssystem-Anbieters zeigt.

Die Selbstauskunft stellt Ihr „Vertrauensprofil“ für eine vereinbarungsgemäße Geschäftsabwicklung dar.

Als nächstes stellt sich für Sie die Aufgabe, Ihr Vertrauensprofil dem Kunden über Ihre Web-Präsenz glaubhaft zu vermitteln (→ Schritt 3).

Hierzu bieten sich eine Reihe von Möglichkeiten an:

- Kleine vertrauensbildende Maßnahmen können Sie direkt an den entsprechenden Stellen in Ihrer Web-Site integrieren. Ein Beispiel hierfür ist die deutliche Kennzeichnung von muss- und kann-Feldern bei der Benutzereingabe.
- Umfangreichere Informationen zu einem Themenpunkt können Sie dem Benutzer hinter einem Informations-Button anbieten. Vorteil: Ihre Web-Seite wird nicht mit Informationen überfrachtet und der Benutzer kann selbst entscheiden, ob er sich die Informationen ansehen möchte. Sie können zum Beispiel auf der Bezahlseite einen Button „Sicherheit beim Zahlen“ anbringen, hinter dem Sie den Kunden über sämtliche von Ihnen getroffenen Maßnahmen und Vorkehrungen informieren.
- Sie fassen das Vertrauensprofil Ihrer gesamten Web-Site in einer Selbstverpflichtungserklärung (disclosure) zusammen, die Sie an einer geeigneten Stelle auf Ihrer Web-Site zugänglich machen.
- Sie lassen Ihre Web-Site (im Fall des WebTrust-Siegels durch Wirtschaftsprüfer) zertifizieren und platzieren das erworbene Siegel deutlich sichtbar auf Ihrer Homepage (Beispiel: www.airmiles.ca).

**Prüfsiegel für
vertrauens-
würdigen
E-Commerce**

Die Preise für Web-Siegel sind sehr unterschiedlich. Das WebTrust-Siegel gehört sicher zu den teuren Siegeln. Einen Überblick über die in Deutschland angebotenen Siegeln finden Sie in der Maiausgabe 2001 der Zeitschrift CYbiz [CAL01].

4 Liste Diensteanbieter für Internet-Zahlungssysteme

4.1 Anbieter von Internet-Zahlungssystemen

Firstgate click&buy

Inkassosystem mit Abrechnung über das Girokonto.

Anbieter:

FIRSTGATE Internet AG
Im MediaPark 5
50670 Köln
Telefon: 0221- 45 45 700
Telefax: 0221- 45 45 710
E-Mail: info@firstgate.de
<http://www.firstgate.de>

GeldKarte

Zahlungssystem mit Chipkarte.

Anbieter:

Sparkassen
<http://ecommerce.sparkasse.de>

infin Micorpayment

Inkassosysteme mit Abrechnung über die Telefonrechnung.

Anbieter:

infin - Ingenieurgesellschaft für Informationstechnologien
mbH & Co. KG
Aidenbachstrasse 141
81479 München

Telefon: 089-745152-0
Telefax: 089-745152-500
E-Mail: fax.voice@infin.de
<http://www.infin.de>

Kontopass net900

Inkassosystem mit Abrechnung über das Girokonto.

Anbieter:

in medias res
Gesellschaft für Kommunikationstechnologien mbH
Limitenstr. 64 - 78
41236 Mönchengladbach / Rheydt
Telefon: 02166-99 99 0
Telefax: 02166-99 99 800
E-Mail: post@in-medias-res.com
<http://www.in-medias-res.de>

net900 Classic

Inkassosystem mit Abrechnung über die Telefonrechnung.

Anbieter:

in medias res
Gesellschaft für Kommunikationstechnologien mbH
Limitenstr. 64 - 78
41236 Mönchengladbach / Rheydt
Telefon: 02166-99 99 0
Telefax: 02166-99 99 800
E-Mail: post@in-medias-res.com
<http://www.in-medias-res.de>

paybox

Handy-basiertes Zahlungssystem.

Anbieter:

paybox.net AG
Postfach 70 12 06
60562 Frankfurt am Main
Telefon: 06026-99 88 77
Telefax: 06026-99 88 76
E-Mail: info@paybox.net
<http://www.paybox.de>

Payitmobile

Handy-basiertes Zahlungssystem.

Anbieter:

Payitmobile AG
Postfach 20 02 27
60606 Frankfurt
Telefon: 01805-payit88
Telefax: 01802-payitfax
E-Mail: info@payitmobile.de
<http://www.payitmobilde.de>

paysafecard

Prepaid-Karte, im Wert von 50, 100 oder 200 Mark. Zahlung im Internet wird mit der PIN, die auf der Karte „freigerubbelt“ werden muss, autorisiert.

Anbieter:

paysafecard.com Wertkarten Aktiengesellschaft
Niederkasseler Lohweg 18
40547 Düsseldorf
Telefon: 0211-52287-0
Telefax: 0211 52887-099
E-mail: info.kunde@paysafecard.com
<http://www.paysafecard.com>

PurePay

Inkassosystem mit Abrechnung über die Telefonrechnung.

Anbieter:

PurePay AG
Salzmannstraße 152
48159 Münster
Telefon: 0251-2 39 36-0
Telefax: 0251-2 39 36-29
E-Mail: info@purepay.com
<http://www.purepay.de>

Streetcash

Handy-basiertes Zahlungssystem.

Anbieter:

inatec GmbH
Fritz-Seger-Straße 16
04155 Leipzig
<http://www.streetcash.de>

Supercent

Inkassosystem mit Abrechnung über die Telefonrechnung.

Anbieter:

INFOGENIE Europe AG
An den Treptowers 1
12435 Berlin
Telefon: 030-726 102 100
Telefax: 030-726 102 199
E-Mail: sc99@infofenie.de
<http://www.supercent.de>

Teleword

Inkassosystem mit Abrechnung über die Telefonrechnung

Anbieter:

EDV Service Gregor Wersche
Münchener Str. 47
10779 Berlin
Telefon: 030-21 105 32
Telefax: 030-21 47 92 32
E-Mail: info@teleword.de
<http://www.teleworld.de>

X-Diver

Inkassosystem mit Abrechnung über die Telefonrechnung.

Anbieter:

eops Germany GmbH
Am Albertussee 1
40549 Düsseldorf
Telefon: 01803-66 63 83
Telefax: 01803-66 24 53
E-Mail: sales@x-diver.de
<http://www.x-diver.de>

4.2 Payment-Service-Provider

Bibit Internet Zahlungen GmbH

Munscheidstraße 14
45886 Gelsenkirchen
Telefon: 0209-167-1040
Telefax: 0209-167-1041
info.de@bibit.com
<http://www.bibit.de>

EBS electronic billing systems AG

Lilienthalstr. 5
85399 Hallbergmoos
Telefon: 0811-5546 300
Telefax: 0811-5546 136
<http://www.payateurodebit.de/>

Gesellschaft für Zahlungssysteme (GZS)

<http://www.gzs.de>

InterCard AG

Mehlbeerenstrasse 4
82024 Taufkirchen bei München
Telefon: 089-61 445-0
Telefax: 089-61 445-511
clearing@intercard.de
<http://www.intercard.de>

isoft Kommunikationstechnologien GmbH

Malteserstraße 170/172
12277 Berlin
Telefon: 030-72 39 22-0
Telefax: 030-72 39 22-21
filsinger@isoft.de
<http://www.isoft.de>

NetManagement GmbH

Grosse Reichenstrasse 27
20457 Hamburg
Telefon: 040-30184-0
Telefax: 040-30184-100
<http://www.netmanagement.com>

TeleCash Kommunikations-Service GmbH

Theodor-Heuss-Straße 8
D-70174 Stuttgart
Telefon: 0711-16264-0
Telefax: 0711-16264-64
welcome@telecash.de
<http://www.telecash.de>

Wire Card AG

Max-Planck-Straße 3
D-85609 Aschheim bei München
Telefon: 089-21 266-0
Telefax: 089-21 266-222
<http://www.wirecard.com>

Glossar

Acquirer

Händlerbank. Ein Unternehmen, welches Akzeptanzstellen für ein Zahlungsmittel (z.B. die Kreditkarte) akquiriert. Darüber hinaus kann ein Acquirer auch für die Betreuung der Vertragspartner sowie für die Abwicklung von Verträgen und Transaktionen zuständig sein.

Akzeptanzstelle

Ein Händler, der ein Zahlungsmittel (z.B. die Kreditkarte) zur Bezahlung akzeptiert.

Anonymität

Anonymität ist ein Maß dafür, inwieweit die beteiligten Akteure (Kunde, Händler, Bank) bei der Abwicklung einer Zahlungstransaktion ihre persönliche Identität gegenseitig offen legen müssen.

Insbesondere aus Sicht des Kunden ist Anonymität ein wünschenswertes Leistungsmerkmal eines Zahlungssystems. So bleibt beispielsweise bei eCash der Zahlende gegenüber den anderen Teilnehmern (Händler und Banken) vollständig anonym. Bei SET wird zwar die größtmögliche Anonymität für ein Kreditkartenzahlungssystem erreicht, gegenüber der Kreditkartengesellschaft gibt der Kunde aber seine Identität preis.

Authentizität

Authentizität bezeichnet die Eigenschaft, dass die an der Zahlungstransaktion beteiligten Partner (Personen, Organisationen) auch diejenigen sind, für die sie sich ausgeben.

Autorisierung

Überprüfung anhand verschiedener Kriterien, ob eine Transaktion zulässig ist. Ein einfaches Beispiel hierfür ist die Prüfung der Kreditkartennummer oder der PIN. (Im Rahmen eines Risiko-Managements können hierfür auch aufwändigere Verfahren eingesetzt werden.) Je nach Ergebnis der Prüfung wird die Transaktion bewilligt (autorisiert) oder verweigert.

Autorisierungszentrale

Ein Rechenzentrum, welches Transaktionen autorisiert.

Bargeld

Geld, welches - im Gegensatz zum Buchgeld - in materieller Form (Münzen oder Scheinen) vorliegt und als gesetzliches Zahlungsmittel dient.

Blinding

Ein bei eCash verwendetes Verfahren, bei dem die Bank eine elektronische Münze „blind“ unterschreibt, das heißt, ohne beim Signieren die Seriennummer der digitalen Münzen lesen zu können. Dadurch wird verhindert, dass Banken die Geldflüsse aufzeichnen und verfolgen können. Zahlungen bleiben so anonym.

Bonität

Ruf einer Person oder Firma im Hinblick auf ihre Zahlungsfähigkeit und -willigkeit. Zur Prüfung der Bonität können Höhe, Regelmäßigkeit und Sicherheit des Einkommens, die Vermögensverhältnisse sowie Auskünfte über das zurückliegende Zahlungsverhalten dienen. Zur Prüfung der Bonität bezüglich einer bestimmten Person wird in der Regel auf Dienstleister, wie zum Beispiel die Schufa, zurückgegriffen.

Buchgeld

Giralgeld oder Depositengeld. Im Gegensatz zu Bargeld, das in Form von Noten oder Münzen im Umlauf ist, bezeichnet man die auf Kontokorrent oder Girokonten stehenden Guthaben (Sichteinlagen) als Buchgeld. Dieses entsteht durch Einzahlung, Überweisung oder Scheck-Gutschrift, aber auch durch Inanspruchnahme vereinbarter Kredite.

Chipkarte

Meist aus Kunststoff bestehende Karte, die mit einem von Computern her bekannten Mikroprozessor (Chip) ausgestattet ist. Dieser Prozessor ist so flach, dass er sich leicht in das Kartenformat integrieren lässt. Ermöglicht der Chip in erster Linie das Speichern von Daten und Werten, so spricht man von einer Speicherkarte (Beispiel: Telefonkarte), gestattet der Chip aber auch das Ausführen von Funktionen, wie zum Beispiel das Verschlüsseln und Entschlüsseln von Daten, so bezeichnet man diese Chipkarten auch als

Smartcards („intelligente Karten“). Ein bekanntes Beispiel für die Smartcard im Bereich der Zahlungssysteme ist die Geldkarte.

Clearing

Periodische Abrechnung im Zahlungsverkehr zum Ausgleich von Forderungen und Verbindlichkeiten zwischen zwei oder mehreren Teilnehmern (z.B. Händler und Bank) mit dem Ziel, dass nur die sich ergebenden Salden gutgeschrieben bzw. belastet werden müssen.

Digitale Güter

Produkte, welche in elektronischer Form vorliegen und zum Verkauf angeboten werden. Beispiele für digitale Güter sind Musikstücke, Spiele, Informationen, Filme. Digitale Gütern spielen für den Verkauf im Internet eine besondere Rolle, da ihre Auslieferung genauso wie ihre Bestellung – im Gegensatz zu physischen (atomaren) Waren – ohne Medienbruch über das Internet erfolgen kann. Mit dem Verkauf von digitalen Gütern sind hohe Anforderungen an die Zahlungssysteme verbunden, da mit der Lieferung möglichst zeitnah die Gegenleistung für den Händler sichergestellt sein soll.

Digitale Unterschrift

Ein Verfahren, das mit kryptografischen Methoden die manuelle Unterschrift für das Internet digital nachbildet. Mit der digitalen Unterschrift wird zum einen die Identität eines Unterzeichners von einem elektronischen Dokument sichergestellt. Zum anderen wird zusätzlich die Authentizität (Gültigkeit und Unverfälschtheit) des Dokumentes gewährleistet. Dies ist mit der digitalen Unterschrift - im Gegensatz zur manuellen Unterschrift - deshalb möglich, da das unterschriebene Dokument fest mit der digitalen Unterschrift verbunden ist.

Digitales Geld

Bei digitalem Geld werden die grundlegenden Eigenschaften des realen Geldes nachgebildet, welches dann in seiner Funktion als Zahlungsmittel dem Bargeld entspricht.

Disagio

Abschlag. Umsatzabhängige Gebühr für eine Transaktion, die der Händler an den Betreiber eines Zahlungssystems abführt.

Double Spending

Das Kopieren und die mehrmalige Verwendung von digitalem Geld wird als „doppeltes Ausgeben“ (double spending) bezeichnet. Diese faszinierende Eigenschaft ist bei digitalem Geld (wie auch beim üblichen Geld) nicht erwünscht. Daher werden Mechanismen eingesetzt, die die einmalige Verwendung sicherstellen. Bei eCash wird hierzu jede elektronische Münze mit einer Seriennummer versehen, mit deren Hilfe geprüft werden kann, ob eine digitale Münze ein zweites Mal im System eingelöst wird.

Duale Signatur

Die duale Signatur ist eine spezielle Ausprägung der digitalen Signatur, bei welcher in einem Vorgang zwei Nachrichten (Auftrags- und Zahlungsanweisung) digital unterschrieben werden. Hierdurch wird sichergestellt, dass bei der Abwicklung einer SET-Zahlungstransaktion der Bezug zwischen Kreditkartendaten und Auftragsanweisung für Händler und Bank jederzeit hergestellt werden kann. Zur Wahrung der Anonymität bleiben aber die Kreditkartendaten dem Händler und die Auftragsdaten der Bank verborgen.

EC-Lastschriftverfahren

Elektronisches Zahlungssystem im Ladengeschäft, bei welchem der Kunde mit Vorlage seiner EC-Karte bezahlt und dem Lastschrifteinzug per Unterschrift zustimmt.

electronic cash

Elektronisches Zahlungssystem im Handel und Dienstleistungsgewerbe, bei welchem der Kunde mittels EC-Karte an einem entsprechenden Händlerterminal bezahlt und die Zahlungsabbuchung per PIN autorisiert.

Electronic Commerce

Es gibt eine Vielzahl von Definitionen dieses Begriffes. Will man ihn weit fassen, so kann man unter Electronic Commerce alle Formen der elektronischen Geschäftsabwicklung unter Verwendung elektronischer Medien verstehen.

Elektronische Geldbörse

Wallet. Digitale Nachbildung der realen Geldbörse zur Aufbewahrung von digitalem Geld bzw. Werteinheiten in Form einer Software (wie z.B. bei eCash) oder einer Chipkarte (wie z.B. bei der Geldkarte). Zudem sind in der

elektronischen Geldbörsen Funktionen integriert, die den Bezahlvorgang unterstützen. Dazu gehört beispielsweise die Zugangskontrolle oder das Aufladen von Werteinheiten.

E-Payment

Eine Zahlung, die auf elektronischem Wege abgewickelt wird.

Evidenzzentrale

Eine Einrichtung, die in einer zentralen Datei Informationen aus verschiedenen Quellen sammelt, zusammenfasst, auf ein bestimmtes Ziel hin überprüft und das Ergebnis zurückmeldet.

Im Fall der Geldkarte wird von den Banken beispielsweise eine Börsenevidenzzentrale betrieben, die Geldkarten-Schattenkonten führt und alle notwendigen Sicherheitsprüfungen vornimmt (z.B. bezüglich Einreichungen gefälschter und verfälschter Umsätze, Mehrfacheinreichungen von Umsätzen).

Weitere Beispiele sind die Kreditprüfung der Deutschen Bundesbank (für Kredite ab drei Millionen Mark) oder die Schufa (Schutzgemeinschaft für allgemeine Kreditversicherung).

Geld

Aus Meyers Lexikon: Allgemeines Tauschmittel, das durch seine Funktion, gegen alle Waren tauschbar zu sein, in einer arbeitsteiligen Wirtschaft unentbehrlich ist. Es dient 1. als Zahlungsmittel; 2. als Recheneinheit, indem es alle bewertbaren Güter vergleichbar macht; 3. als Mittel zur Wertspeicherung, mit dessen Hilfe der Tausch von Gütern zeitlich versetzt stattfinden kann.

GeldKarte

Zahlungssystem, welches auf einer Chipkarte basiert und zur Bezahlung digitales Geld bzw. Werteinheiten einsetzt. Die Geldkarte gibt es als kontogebundene Karte (kleiner goldener Chip auf den Kunden- bzw. EC-Karten) und als kontoungebundene Karte, mit welcher anonyme Zahlungen möglich sind.

HBCI (Home Banking Computer Interface)

Standard für das Online-Banking mit dem Ziel, dem Kunden den vollen Leistungsumfang (z.B. Daueraufträge, Sammelaufträge, Terminüberweisung)

gen, Festgeldanlage oder Wertpapierorder) der Kreditinstitute über ein Kommunikationsnetz (z.B. Internet) zur Verfügung zu stellen.

Inkasso

Inkasso bedeutet ganz allgemein der Einzug von Forderungen. Im Bankenbereich ist zum Beispiel die Abwicklung von eingereichten Schecks oder Lastschriften ein Inkassovorgang. Inkassosysteme im E-Payment-Bereich sammeln Zahlungsbeträge über einen bestimmten Zeitraum und ziehen diese dann über das Girokonto oder die Telefonrechnung ein.

Internet-Shop

Internet-Seiten, auf denen ein Unternehmen Produkte und/oder Dienstleistungen anbietet und den Verkauf dieser (möglichst weitgehend) abwickelt.

Issuer

Emittent oder Kundenbank. Unternehmen, welches für die Ausgabe der jeweiligen Kreditkarten im Auftrag der Kreditkartengesellschaften an die Endkunden verantwortlich ist.

Kontogebundenes Zahlungssystem

Eine Transaktion im elektronischen Zahlungssystem wird auf eine Transaktion im konventionellen Kontensystem abgebildet (Beispiele: paybox, Kreditkartenzahlung).

Kontungebundenes Zahlungssystem

Die Durchführung von Zahlungstransaktionen im elektronischen Zahlungssystem basiert nicht auf Transaktionen im konventionellen Kontensystem. Für die Benutzung der Geldkarte beispielsweise ist es nicht notwendig, auch ein Girokonto zu besitzen.

Kreditkarte

Plastikgeld. Karte, die ihren Inhaber berechtigt, bei Akzeptanzstellen wie Einzelhandelsgeschäfte, Hotels, Reisebüros, Waren und Dienstleistungen bargeldlos einzukaufen. Kreditkarten sind für den Kreditkarteninhaber ein weltweit einsetzbares Zahlungsmittel.

Macropayment

Bezeichnung für Zahlungsvorgänge mit Beträgen deutlich über 10,- DM.

Micropayment

Bezeichnung für Zahlungsvorgänge mit Beträgen unter 10,- DM. Kleinstzahlungen (unter 1,- DM) werden als Picopayments bezeichnet. Nur wenige E-Payment-Systeme sind für kleinere Zahlungen geeignet, da die Transaktionskosten unverhältnismäßig ins Gewicht fallen.

Offline-Zahlung

Bei der Offline-Zahlung erfolgt die Bezahlung ohne Verwendung elektronischer Kommunikationsmedien. Der Kauf auf Rechnung oder die Nachnahme sind Beispiele für Offline-Zahlungen. Beim Einkauf über das Internet geht die Offline-Zahlung daher mit einem Medienbruch einher.

Online-Banking

Electronic-Banking. Mit Online-Banking wird eine Vielzahl von Bankdienstleistungen bezeichnet, die es dem Kunden ermöglichen, seine Bankgeschäfte von Zuhause aus durchzuführen, ohne persönlich in der Geschäftsstelle erscheinen zu müssen.

Online-Zahlung

Bei der Online-Zahlung werden für die Abwicklung der Bezahlung elektronische Kommunikationsmedien eingesetzt.

Alle Internet-Zahlungssysteme sind Beispiele für Online-Zahlungssysteme. Wird die Bestellung, die Bezahlung sowie im Fall digitaler Waren auch die Lieferung über das Internet vorgenommen, so ist ein medienbruchfreier E-Commerce realisiert.

Payment-Service-Provider (PSP)

Dienstleistungs-Unternehmen, welches den Vorgang der elektronischen Bezahlung vollständig oder teilweise für den Händler abwickelt. Zusätzlich können Payment-Service-Provider weitergehende Dienstleistungen anbieten, wie z.B. Vertragsabschluss, Inkassoverfahren, Aufbereitung der Zahlungsdaten.

PIN (Personal Identification Number)

Die PIN ist eine persönliche Geheimnummer, die ähnlich einem Passwort eingegeben werden muss, bevor der Zugang zu einem persönlichen Dienst (z.B. das Abheben von Bargeld an Geldautomaten) freigeschaltet wird.

POS (Point of Sale)

Verkaufsstelle, wie zum Beispiel das Ladengeschäft, wo der reale Verkauf von Waren stattfindet.

Scheck

Mit der Ausstellung eines Schecks weist der Kontoinhaber seine Bank an, dem Überbringer einen bestimmten Betrag auszuzahlen. Bei Schecks mit dem Vermerk "Nur zur Verrechnung" darf der Betrag lediglich auf ein Konto gutgeschrieben werden und ist damit gegen Diebstahl und Unterschlagung (eingermaßen) gesichert.

Beim Scheck handelt es sich um ein empfängerinitiiertes Bezahlverfahren.

SET (Secure Electronic Transaction)

Standard zur Abwicklung von Kreditkartentransaktionen über das Internet.

Sperrlisten

Meist vom Handel geführte Listen von Karten, deren Nutzung nicht mehr zulässig ist.

SSL (Secure Socket Layer)

Ein von der Firma Netscape entwickeltes Verfahren zur verschlüsselten Datenübertragung über das Internet. Neben der Verschlüsselung unterstützt SSL auch die Authentifizierung der Kommunikationspartner per Zertifikate.

SWIFT-Netz

Society for Worldwide Interbank Financial Telecommunication. SWIFT ist eine Organisation mit ca. 1580 Mitgliedern, überwiegend Banken und Börsen aus 70 Ländern, die ein bankeneigenes Computernetzwerk betreiben, um Banktransaktionen abzuwickeln. Das SWIFT-Netz genügt Sicherheitsanforderungen; insbesondere ist es im Gegensatz zum Internet nicht allgemein zugänglich.

TAN (Transaction Access Number)

Die TAN ist eine Geheimnummer zur Freischaltung einer einzelnen Transaktion und wird häufig beim traditionellen Online-Banking eingesetzt. Der Bankkunde erhält hierbei von seiner Bank eine Liste mit TANs. Jede Überweisung wird mit einer TAN dieser Liste freigeschaltet. Nach einer einmaligen Nutzung ist die TAN ungültig.

Transaktionskosten

Kosten, die bei der Durchführung einer Zahlungstransaktion anfallen. Die Transaktionskosten bestimmen ganz wesentlich, für welche Bereiche sich ein Zahlungssystem einsetzen lässt.

Überweisung

Mit einer Überweisung beauftragt der Kunde sein Kreditinstitut, für ihn eine Zahlung durchzuführen. Das Institut bucht hierbei den zu zahlenden Betrag vom Konto des Auftraggebers ab und überweist ihn auf das angegebene Konto des Empfängers. Bei einer Überweisung handelt es sich, im Gegensatz zur Einzugsermächtigung, um einen absenderinitiierten Bezahlvorgang.

Verschlüsselung

Bei der elektronischen Verschlüsselung werden die Daten im System des Absenders vor der Übertragung über das Internet codiert (verschlüsselt) und erst beim Empfänger wieder in einem System decodiert (entschlüsselt), so dass die Daten bei der Übertragung von unberechtigten Personen nicht gelesen werden können. Die Sicherheit einer Verschlüsselung hängt zum einen von den verwendeten Verschlüsselungsverfahren und Schlüssellängen ab, zum anderen ganz wesentlich von der Konzeption des Gesamtsystems (so nützt es wenig, für die Datenübertragung ausgefeilte kryptografische Verfahren zu verwenden, wenn die Daten dann nach ihrer Entschlüsselung offen auf einem ungeschützten System gespeichert werden).

Bei der Bezahlung im Internet spielt die Verschlüsselung eine wesentliche Rolle, da es sich hierbei um besonders sensible Daten (z.B. die Kreditkartennummer) handelt.

Zentraler Kreditausschuss (ZKA)

Arbeitsgemeinschaft der Spitzenverbände der Kreditwirtschaft, welche sich aus dem Deutschen Sparkassen- und Giroverband (DSGV), dem Bundes-

verband der Deutschen Volks- und Raiffeisenbanken (BVR), dem Bundesverband deutscher Banken (BdB) und dem Verbund öffentlicher Banken (VÖB) zusammensetzt. Die ZKA dient der Abstimmung brancheneinheitlicher Regelungen zu allen wichtigen Geldinnovationen (z.B. Spezifizierung und Einführung von electronic cash oder der Geldkarte).

Zertifikate

Zertifikate spielen bei der Verwendung asymmetrischer Verschlüsselungsverfahren eine bedeutende Rolle. Ein Zertifikat ordnet hierbei einen öffentlichen Schlüssel eindeutig einer Person oder Institution zu. Diese Zuordnung wird durch eine Zertifizierungsstelle garantiert. Wird eine Internetverbindung beispielsweise mit SSL verschlüsselt, so kann der Kunde über das Zertifikat nachprüfen, mit wem die Kommunikationsverbindung besteht. Die Vertrauenswürdigkeit der Zertifizierungsstelle ist ausschlaggebend für die Aussagekraft eines Zertifikats.

Anmerkung:

Asymmetrische Verschlüsselungsverfahren verwenden zwei zueinander gehörige Schlüssel: (a) den geheimen Schlüssel, den nur der Berechtigte (etwa in Form einer Chipkarte) besitzt und (b) den öffentlichen Schlüssel, der allgemein bekannt gegeben wird. Die Sicherheit asymmetrischer Verschlüsselungsverfahren basiert wesentlich darauf, dass sich klar nachvollziehen lässt, zu wem ein öffentlicher Schlüssel gehört.

Zertifizierungsstelle

Trust Center, Certification Authority. Dienstleistungsunternehmen, welches die Identität von Antragstellern prüfen und ihnen Zertifikate ausstellen. Bekannte Zertifizierungsstellen sind z.B. Verisign oder Twayte.

Literatur

Alle Internetadressen (URLs) sind vom Stand: 10. Juni 2001.

- [AICPA1] AICPA/CICA: WebTrust^{SM/TM} Program, Program for Online Privacy, Version 3.0, November 30, 2000.
(http://www.cpawebtrust.org/privacy_fin.htm)
- [AICPA2] AICPA/CICA: WebTrust^{SM/TM} Program, Security Principle and Criteria, Version 3.0, January 1, 2001.
(http://www.cpawebtrust.org/Security_fin.htm)
- [AICPA3] AICPA/CICA: WebTrust^{SM/TM} Program, Availability Principle and Criteria, Version 3.0, January 1, 2001.
(http://www.cpawebtrust.org/avail_fin.htm)
- [AICPA4] AICPA/CICA: WebTrust^{SM/TM} Program, Business Practices / Transaction Integrity Principle and Criteria, Version 3.0, January 1, 2001.
(http://www.cpawebtrust.org/BusPracTrans_fin.htm)
- [BEU99] Beutelsbacher A., Schwenk J., Wolfenstetter K.-D.: Moderne Verfahren der Kryptographie, Vieweg, 3. Auflage, 1999.
- [BEY98] Beykirch Hans-Bernhard: Chipgeld – Wie die GeldKarte funktioniert, iX 12/98.
- [BÖH00] Böhle Knud, Riehm Ulrich, Wingert Bernd: Benutzungsaspekte von Bezahlsoftware im Internet, Forschungszentrum Karlsruhe, Institut für Technologieabschätzung und Systemanalyse (ITAS), 1999.
(<http://www.itas.fzk.de/deu/Itaslit/boua99a.pdf>)
- [BRA99] Braatz Frank, Brinker Ulrich, Friederich Hans-Jürgen: Alles über Zahlungsverkehr mit Karten, Luchterhand Verlag 1999.
- [BUN] Bundeskartellamt, Nachrichten: „Bundeskartellamt mahnt Einführung eines Interbankentgeltes für Zahlungen mit der EC-Karte an“.
(http://www.bundeskartellamt.de/07_03_2001.html)
- [CAL01] Calik Kemal: Vertrauenssache – Zertifikate sollen Online-Geschäfte sicherer machen, CYbiz, Mai 2001.
- [COM] Commerzbank: SET – Informationen zum Eurocard/Mastercard Pilotprojekt der Commerzbank.
(http://www.commerzbank.de/privat/service/set_pilot.html)

- [CYB] CyberCash: WebPOS.
(<http://www.cybercash.de/posh/index.html>)
- [EBE97] Eberl Markus, Färber Johannes, Schuster Rolf: Digital Cash, Springer Verlag, 1997.
- [ECA] eCash. (<http://www.ecash.com/online/>)
- [ECE] Electronic Commerce InfoNet: Zahlungssysteme.
(<http://www.ecin.de>)
- [FUW97] Furche Andreas, Wrightson Graham: Computer Money, dpunkt-Verlag, 1997.
- [GEN97] Gentz Wolfgang: Die elektronische Geldbörse in Deutschland: Funktionsweise, Kosten und Nutzen für die Beteiligten, Diplomarbeit an der Fachhochschule München, 1997.
(<http://www.ubkoch.de/index2.html>)
- [GRI00] Grill Wolfgang, Percynski Hans: Wirtschaftslehre des Kreditwesens, Verlag Gehlen, 2000.
- [HEN01] Henkel, Joachim: Bezahlen auf Draht – E-Payment: Wie der Rubel ins Rollen kommt, c't 6/01.
- [INM] in media res: net900. (<http://www.in-media-res.com>)
- [INT] Internet-Recht: Sammlung von Rechtsvorschriften im Internet, „EU-Signaturrichtlinie und Umsetzung“.
(<http://www.internetrecht-info.de>)
- [Ket01] Ketterer, Institut für Wirtschaftspolitik und Wirtschaftsforschung - Universität Karlsruhe - Sektion Geld und Währung: Umfrage zu Zahlungsmitteln im Internet vom 15. November 2000 bis zum 31. Januar 2001.
(<http://www.iww.uni-karlsruhe.de/IZV4/auswertung/studie.html>)
- [KRA98] Krause Jörg: Electronic Commerce und Online-Marketing, Hanser-Verlag, 1999.
- [KRI98] Kristoferitsch Georg: Digital Money – Electronic Cash – Smart Cards, Wirtschaftsverlag Ueberreuter, 1998.
- [LEI00] Leischner Martin: E-Cash, Electronic Banking, Summer University Informationssicherheit, St. Augustin, 2000.
- [LEP99] Lepschies Gunter: E-Commerce und Hackerschutz, Vieweg verlag, 1999.
- [LUK95] Lukas Sylvia: Elektronische Zahlungssysteme in Deutschland, Luchterhand Verlag, 1995.

-
- [LUK97] Lukas Sylvia: Cyber Money, Luchterhand Verlag, 1997.
- [LUN96] Lundquist Leslie, Lynch Daniel C.: Zahlungsverkehr im Internet, Hanser Verlag, 1996.
- [PAY] paybox. (<http://www.paybox.de>)
- [PER97] Pernul Günther, Röhm Alexander W.: Neuer Markt – neues Geld? Wirtschaftsinformatik 39/97.
- [RAE98] Raeppele Martin: Sicherheitskonzepte für das Internet, dpunkt-Verlag, 1998.
- [SEE01] Seeger Jürgen: Kritische Masse – Zahlungssysteme im Internet vor dem Durchbruch, iX 3/01.
- [SEL00] Selke Gisbert W.: Kryptographie, O'Reilly, 2000.
- [SET197] SETCo: SET Secure Electronic Transaction Specification, Book 1: Business Description, Version 1.0, May 1997.
(www.setco.org)
- [SET297] SETCo: SET Secure Electronic Transaction Specification, Book 2: Programmer's Guide, Version 1.0, May 1997.
(www.setco.org)
- [SET397] SETCo: SET Secure Electronic Transaction Specification, Book 3: Formal Protocol Definition, Version 1.0, May 1998.
(www.setco.org)
- [SIE97] Sietmann Richard: Electronic Cash, Schäffer-Poeschel Verlag, 1997.
- [SPA] Sparkasse: GeldKarte und SET.
(<http://www.sparkasse.de/ecommerce>)
- [STO97] Stolpmann Markus: Elektronisches Geld im Internet, O'Reilly, 1997.
- [TÖP00] Töpfer Alfred: Confidence in e-commerce?, Stiftung Warentest Office Berlin, 2000.
(http://europa.eu.int/comm/dgs/health_consumer/events/event32_wrks4-1_de.html)
- [WEB] WebPOS (<http://www.webpos.de>).
- [WEI92] Weimar Wolfram: Geschichte des Geldes, Insel Verlag, 1992.

Index

- 3D-SET 35
- Acquirer 19, 87
- Akzeptanzstelle 19, 38, 87
- Alphacodes 23
- Anonymität 62, 87
- Authentizität 62, 87
- Autorisierung 87
- Autorisierungszentrale 88
- Bargeld 88
- blinding 56
- Blinding 88
- Bonität 88
- Börsenevidenzzentrale
- Buchgeld 88
- Card Verification Code 23
- Chipkarte 88
- Clearing 89
- CVC2 23
- CyberCash 26
- digitale Güter 89
- digitale Münzen 55
- digitale Unterschrift 89
- digitales Geld 89
- Disagio 89
- Double Spending 90
- duale Signatur 90
- eCash 55
- EC-Lastschriftverfahren 90
- Einreichergebühr 43
- electronic cash 90
- Electronic Commerce 90
- Elektronische Geldbörse 90
- E-Payment 91
- Evidenzzentrale 91
- Geld 91
- GeldKarte 36, 91
- Händlervidenzzentrale 38
- HBCI 91
- HBCI-Standard 37
- infin Micropayment 49
- Inkasso 92
- Internationalität 65
- Internet-Shop 92
- Issuer 19, 92
- Kartenevidenzzentrale *Siehe*
 - Börsenevidenzzentrale
- Kartenprüfnummer 23
- kontogebundenes Zahlungssystem 92
- kontungebundenes Zahlungssystem 92
- Kreditkarte 92
- Kundenakzeptanz 61
- Macropayment 93
- Micropayment 93
- MOTO-Vertrag 23
- Nachvollziehbarkeit 64
- net900 Classic 49
- net900 Kontopass 50
- Offline-Zahlung 93
- Online-Banking 93
- Online-Zahlung 93
- Pay per Call 50
- Pay per Minute 50
- paybox 44
- paybox-PIN 47
- Payment-Service-Provider 93
- Personal Identification Number 94
- PIN 11 *Siehe* Personal Identification Number
- Point of Sale 94
- POS 94 *Siehe* Point of Sale
- PSP *Siehe* Payment Service Provider
- Schattenkonto 37
- Scheck 94
- Secure Electronic Transaction 94
- Secure Socket Layer 94
- SET 30 *Siehe* Secure Electronic Transaction
- SETCo 31
- SET-Zertifikat 30
- SIM-Karte 47
- Sperrlisten 94
- SSL 94
- SWIFT-Netz 94
- TAN *Siehe* Transaction Access Number

Transaction Access Number 95
Transaktionsbearbeitung 64
Transaktionskosten 95
Überweisung 95
unblinding 56
Universalität 65
Verfügbarkeit 75
Verschlüsselung 95
Vertraulichkeit 62
VU-Nummer 22
Wallet 33

WebPOS 26
weiße Karten 37
X-Diver 49
Zahlungsausfälle 64
Zahlungssicherheit 63
Zeitpunkt der Gutschrift 63
Zentraler Kreditausschuss 36, 95
Zertifikat 96
Zertifizierungsstelle 96
ZKA *Siehe* Zentraler Kreditausschuss

