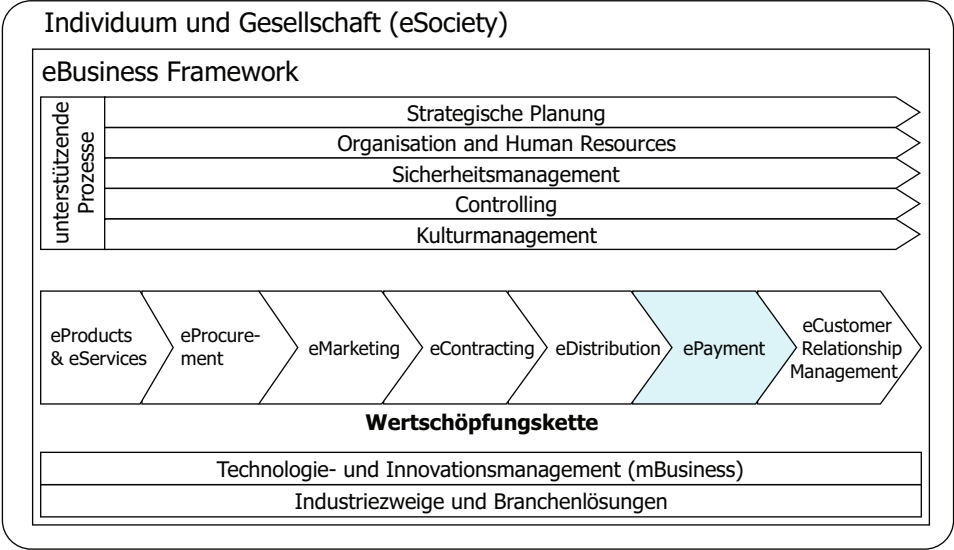


Zusammenfassung

Das Kapitel ePayment beleuchtet den elektronischen Zahlungsverkehr. Im Abschn. 7.1 wird ein Klassifikationsschema vorgestellt, mit dem sich Payment-Lösungen einordnen lassen. Abschnitt 7.2 illustriert mit der Kreditkarte das heute beliebteste Zahlungsmittel im elektronischen Zahlungsverkehr und beschreibt die darauf aufbauenden Verfahren PayPal und SET (Secure Electronic Transaction). Abschnitt 7.3 stellt guthabenbasierende Verfahren vor. Abschnitt 7.4 zeigt innovative Lösungen aus den 90er-Jahren, die sich im Markt nicht durchsetzen konnten. Spezielle Lösungen für eShop-Betreiber werden in Abschn. 7.5 behandelt. Abschnitt 7.6 konzentriert sich auf Lösungen zum Bezahlen kostenpflichtiger Webseiten. Ein Vergleich von heute genutzten, unterschiedlichen Payment-Systemen findet sich in Abschn. 7.7, bevor das Kapitel in Abschn. 7.8 mit Literaturhinweisen schliesst.



7.1 Überblick und Klassifikation

Unter dem Begriff ePayment versteht man die elektronische Abwicklung von Zahlungsvorgängen. Eine Person oder Institution kann einen Geldbetrag elektronisch an einen Empfänger senden. Mit ePayment wird beispielsweise ein Produkt bezahlt, welches in einem Online-Shop gekauft wurde.

Für das ePayment existieren Lösungen, welche sich auf verschiedene Arten klassifizieren lassen:

- Wie hoch ist der Betrag?

Höhe des Betrags ePayment-Lösungen lassen sich über die Höhe des Betrags klassifizieren. Es existieren die drei Klassen Picopayment, Micropayment und Macropayment. In der Picopayment-Klasse finden sich Lösungen für kleine Beträge (weniger als 1 Cent bis 1 Euro). Solche Lösungen sind beispielsweise für den Betrieb einer kostenpflichtigen Webseite geeignet. Um die Webseite anzusehen bezahlt eine Person einen kleinen Betrag von etwa 10 Cent. Die Micropayment-Klasse enthält Payment-Lösungen zwischen 1 Euro und 10 Euro. Payment-Lösungen für grössere Beträge werden in die Macropayment-Klasse eingestuft. Eine solche Klassifizierung ist sinnvoll, da je nach Zielmarkt unterschiedliche Anforderungen bestehen. Je höher der Betrag, desto grösser muss die Sicherheit sein. Lösungen für Picopayment sollten einfach zu handhaben sein, da ein Benutzer nicht für jeden Kleinstbetrag umständliche Eingaben tätigen will.

- Wann wird bezahlt?

Zeitpunkt der Zahlung Der Zeitpunkt der Transaktion wird zur Klassifikation von Payment-Lösungen herangezogen. Hierbei lässt sich zwischen den Klassen Pre-Paid, Pay-Now und Pay-Later unterscheiden. Bekannte nicht elektronische Payment-Beispiele sind Vorkasse für Pre-Paid, Nachnahme für Pay-Now sowie Rechnung für Pay-Later.

- Wie wird die Lösung realisiert?

Technologisches Konzept Payment-Lösungen lassen sich über die eingesetzten Technologien unterscheiden. Mögliche Klassen differenzieren zwischen der Abrechnung und der Art der Speicherung des elektronischen Geldes. Dieses wird auf einem Konto abgelegt oder in Form von virtuellen Münzen in Software oder Hardware gespeichert.

- Kennt der Verkäufer oder die Bank den Käufer?

Anonymität Payment-Lösungen unterscheiden sich anhand der Anonymität. Beahlt eine Person im nicht elektronischen Zahlungsvorgang ein Produkt mit Bargeld, handelt es sich um eine anonyme Transaktion. Bei der Kreditkarte ist die Transaktion nicht anonym,

weil der Verkäufer den Namen des Käufers kennt. Für das ePayment existieren sowohl anonyme als auch nicht anonyme Lösungen.

Im Folgenden werden einige ePayment-Lösungen vorgestellt.

7.2 Kreditkartenbasierte Verfahren

Die meisten erfolgreichen ePayment-Lösungen basieren auf Kreditkarten, die bereits im Offline-Handel ein beliebtes Zahlungsinstrument darstellen. Im Folgenden wird zunächst eine direkte Lösung vorgestellt. Anschliessend folgt eine kurze Einführung in PayPal, das mit mehr als 140 Millionen registrierten Kunden derzeit eine der beliebtesten ePayment-Lösungen darstellt. Schliesslich zeigt die SET-Lösung auf, dass es möglich ist, eine sichere Online-Zahlungsmethode zu entwickeln. Allerdings konnte sich SET aufgrund der grossen Voraussetzungen, die es an die Nutzer stellt, in der Praxis nicht durchsetzen.

7.2.1 Kreditkarten mit Secure Socket Layer (SSL)

- Secure Socket Layer für eine sichere Verbindung

Kreditkarten sind als Zahlungsmittel im ePayment beliebt, wobei üblicherweise grössere Beträge bezahlt werden (Macropayment). Die Zahlung erfolgt mit der auf der Karte aufgedruckten Nummer. Damit diese nicht im Internet abgelauuscht werden kann, erfordert die Übermittlung eine sichere Leitung. In den letzten Jahren hat sich im Online-Handel die Annahme von Kreditkarten über eine SSL (Secure Socket Layer) verschlüsselte Verbindung etabliert. Das SSL-Protokoll ist in den meisten Browsern verfügbar und erstellt eine verschlüsselte Verbindung zwischen dem Client (dem Browser des Kunden) und dem Server (dem Anbieter). Dazu wird auf eine Reihe von kryptographischen Verfahren zurückgegriffen (vgl. Abschn. 5.3).

- Gründe für die Popularität von Kreditkarten

Für die Popularität von Kreditkarten lassen sich folgende Gründe ausmachen:

- Kreditkarten sind im Offline-Handel bereits seit Jahrzehnten im Einsatz.
- Kreditkarten sind weltweit verfügbar und akzeptiert.
- Kreditkarten sind einfach in der Handhabung und benötigen keine spezielle Software. Für die Online-Zahlung muss lediglich die Kreditkartennummer mit dem Namen des Karteninhabers in ein Formular eingegeben werden.
- Kreditkarten sind für den Käufer in der Regel günstig. Viele Banken berechnen eine geringe Grundgebühr und locken bei entsprechendem Umsatz mit weiteren Rabatten oder Prämien.



Abb. 7.1 Rückseite einer Kreditkarte mit der Kartenprüfnummer 999

► Nachteile von Kreditkarten

Allerdings haben Kreditkarten auch einige Nachteile:

- Kreditkarten besitzen keinerlei Sicherheitsmechanismen. Stiehlt ein Angreifer eine Kreditkartennummer, genügt diese, um damit online einzukaufen. Im Online-Handel wird deshalb von einigen Anbietern neben der Kreditkartennummer eine dreistellige Kartenprüfnummer (Sicherheitscode) verlangt (siehe Abb. 7.1). Diese soll das Betrugsrisiko reduzieren, da die Kartenprüfnummer auf keinem Beleg (Rechnung des Kreditkartenunternehmens, Zahlungsanweisung, etc.) auftaucht. Allerdings ist der Erfolg dieser Massnahme mässig, da diese Nummer auf der Rückseite der Kreditkarte aufgedruckt ist und somit beim Bezahlen für jeden einsehbar ist.
- Kreditkarten sind nicht anonym. Beim Kauf eines Produkts erfahren sowohl Verkäufer als auch abwickelnde Banken die Kreditkartennummer, was wiederum ein Sicherheitsrisiko darstellt.
- Kreditkarten eignen sich nicht für Zahlungen zwischen privaten Personen. Damit eine Person über eine Kreditkarte Geld empfangen kann, muss sie mit einem Kreditkartenunternehmen bzw. einer Bank einen besonderen Vertrag abschliessen.
- Kreditkarten sind für den Verkäufer teuer. Kreditkarteninstitute und Banken verlangen von ihm relativ hohe Grundgebühren sowie einen prozentualen Umsatzanteil.

Trotz der hier aufgezeigten Mängel hat sich die Kreditkarte beim ePayment als Zahlungsmethode durchgesetzt.

7.2.2 PayPal

Das Unternehmen PayPal wurde im Jahr 1998 als selbstständiges Unternehmen gegründet und 2002 vom Auktionshaus eBay übernommen. PayPal ist ein kreditkartenorientiertes Zahlungssystem. Es ermöglicht, im Gegensatz zum oben beschriebenen direkten Einsatz von Kreditkarten, Zahlungen zwischen zwei Privatpersonen. Als US-amerikanisches Unternehmen bot PayPal lange Zeit nur eine Abrechnung in US-Dollar an, mittlerweile werden mehr als 15 weitere Währungen, darunter Euro, britisches Pfund und Schweizer Franken, unterstützt.

► Registrierungsprozess

Um PayPal nutzen zu können, ist eine Registrierung notwendig. PayPal setzt ein einfaches aber effektives Mittel ein, um sich vor Kreditkartenmissbrauch zu schützen: Ein neu registrierter Benutzer gibt seine Kreditkarteninformationen ein, kann jedoch PayPal noch nicht benutzen, da das Konto noch nicht aktiviert ist. Anschliessend bucht PayPal von der eingegebenen Kreditkarte einen kleinen Betrag ab (normalerweise 1 Dollar). In der Beschreibung der Abbuchung ist eine Nummer zu finden. Der Benutzer kann diese Nummer auf seiner Kreditkartenabrechnung lesen und sie bei PayPal eingeben, um das Konto zu aktivieren. Durch diese Methode ist es schwierig, eine gestohlene Nummer bei PayPal zu registrieren, da der Dieb normalerweise keinen Zugang zur Kreditkartenabrechnung hat. Hat der Benutzer sich erfolgreich bei PayPal registriert, kann er eine Transaktion zu einem anderen PayPal Mitglied durchführen (siehe Abb. 7.2).

► Beispiel einer PayPal Transaktion

Will eine Person A ein Produkt von einer anderen Person B kaufen, sendet B zunächst die notwendigen Zahlungsinformationen. Dazu gehört der Kontoname, der der eMail-Adresse entspricht, sowie der zu bezahlende Betrag (Schritt 1). Person A authentifiziert sich anschliessend auf dem Web-Server von PayPal und gibt die erhaltenen Zahlungsinformationen in ein Formular ein (Schritt 2). PayPal belastet die Kreditkarte von Person A und schreibt das Geld dem virtuellen Konto des Empfängers gut (Schritt 3 und 4). Mit dem Geld auf diesem virtuellen Konto startet der Empfänger entweder eigene Transaktionen, oder lässt es sich auf ein Bankkonto überweisen. Der Empfänger einer Transaktion bezahlt an PayPal eine Gebühr, die abhängig vom Umsatz ist. Diese wird vom empfangenen Betrag direkt abgebucht. Anschliessend generiert PayPal eine Bestätigungsmail an die Personen A (Schritt 5) und B (Schritt 6). Person B kann jetzt das Produkt an Person A ausliefern (Schritt 7).

► Zur Popularität von PayPal

Die Popularität von PayPal ist eng mit dem Erfolg des Auktionshauses eBay verbunden. Seit der Übernahme durch eBay ist PayPal fest integriert und viele Benutzer von eBay sind

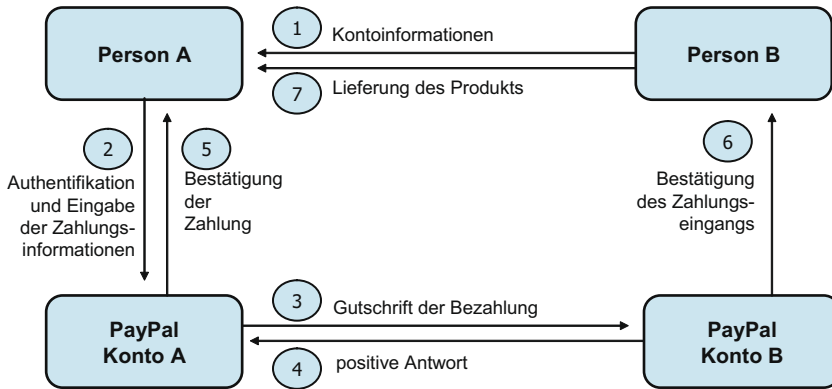


Abb. 7.2 Der PayPal-Zahlungsprozess zwischen zwei Privatpersonen

auch PayPal-Nutzer. eBay fördert die elektronische Zahlung mit PayPal offensiv. Auf der australischen eBay-Seite zum Beispiel werden als Zahlungsmethoden nur noch PayPal und Barzahlung bei Abholung akzeptiert.

Fallbeispiel eDVDShop: Elektronisches Bezahlen mit PayPal

Der eDVDShop bietet zur Zeit als Zahlungsmöglichkeit nur den Nachnahmeversand per Post sowie den Versand per Rechnung. Diese Verfahren eignen sich für den deutschsprachigen Raum. Allerdings steigt die Anzahl internationaler Kunden beim Shop stetig. Marcel Anderson möchte für diese Kunden eine Online-Zahlungsmöglichkeit schaffen.

Nach einigen Recherchen entscheidet er sich für PayPal. Die Integration von PayPal in den Online-Shop ist einfach. Auf der Webseite von PayPal findet er verschiedene Integrationsmöglichkeiten. Er entscheidet sich für die Express Checkout Variante. PayPal stellt einen Wizard bereit, in welchem Anderson alle notwendigen Informationen für die Integration, etwa die Programmiersprache des Online-Shops und die Standardwährung, angeben kann. Aus allen Daten erzeugt der Wizard Quelltext, den er in seinen Online-Shop beim Start des Checkout-Prozesses einfügt. Der erzeugte Quelltext hat in etwa folgendes Aussehen:

```
<form name="_xclick" action="https://www.paypal.com/cgi-bin/webscr"
  method="post">
  <input type="hidden" name="cmd" value="_xclick">
  <input type="hidden" name="business" value="marcel@edvdshop.ch">
  <input type="hidden" name="currency_code" value="EUR">
  <input type="hidden" name="item_name"
    value="eDVDShop: Lola Montez SE">
  <input type="hidden" name="amount" value="15.99">
```

```
<input type="image"
      src="http://www.paypal.com/en_US/i/btn/x-click-but01.gif"
      border="0" name="submit"
      alt="Make payments with PayPal">
</form>
```

Die versteckten Felder muss Anderson mit den korrekten Werten der anstehenden Bezahlung ausfüllen. Als Währung (`currency_code`) wählt er Euro (EUR). Anschliessend setzt er seine eMail-Adresse ein. Die übrigen Daten sind variabel, sie müssen für jede Bestellung dynamisch eingebunden werden. Obiges Beispiel enthält variable Namen, etwa den Produktnamen (`item_name`, im Beispiel eDVDShop: Lola Montez SE) sowie den zu zahlenden Betrag (`amount`, im Beispiel 15.99).

Daneben gibt es weitere Optionen. Beispielsweise lassen sich die Versandkosten (Shipping) gesondert ausweisen. Auch kann über das Attribut `return` eine Rückadresse angegeben werden, auf die der Kunde nach der erfolgreichen Eingabe seiner Zahlungsinformationen geleitet wird. Gleiches gilt, falls der Kunde die Bezahlung abbricht (`cancel-return`).

Obiges Formular integriert Marcel Anderson in seinen Checkout-Prozess. Betrachtet man das Formular im Web-Browser, wird ein Button (siehe `<input type=„image“`) angezeigt. Drückt der Kunde den Button, wird er automatisch auf die PayPal Seite weitergeleitet. Dort muss er sich gegenüber PayPal authentifizieren, um den Zahlungsvorgang zu starten. Da Anderson das `return` Attribut korrekt gesetzt hat, wird der Kunde anschliessend zurück auf die eDVDShop-Seite geleitet, wo ihm für die Bestellung gedankt wird.

7.2.3 Secure Electronic Transaction (SET)

- ▶ SET ist ein sicheres Protokoll

Das SET-Protokoll wurde von einigen grösseren Kreditkartenunternehmen (VISA, Mastercard) in Kooperation mit Technologieunternehmen wie IBM, Microsoft und Netscape entwickelt. SET gilt als eines der sichersten Protokolle im ePayment. Sein Einsatz erfordert eine Reihe von Voraussetzungen aller beteiligten Parteien. Insbesondere basiert SET auf einem Public Key Kryptosystem (siehe Abschn. 5.3). Alle beteiligten Parteien benötigen ein Schlüsselpaar. Diese Bedingung ist bis heute nur lückenhaft erfüllt. Daneben gibt es weitere Voraussetzungen für die beteiligten Parteien:

- ▶ SET-Wallet für den Käufer
- Der Käufer benötigt ein SET-Wallet, eine Art elektronische Geldbörse. Das SET-Wallet speichert die notwendigen Daten und kommuniziert mit dem Verkäufer.

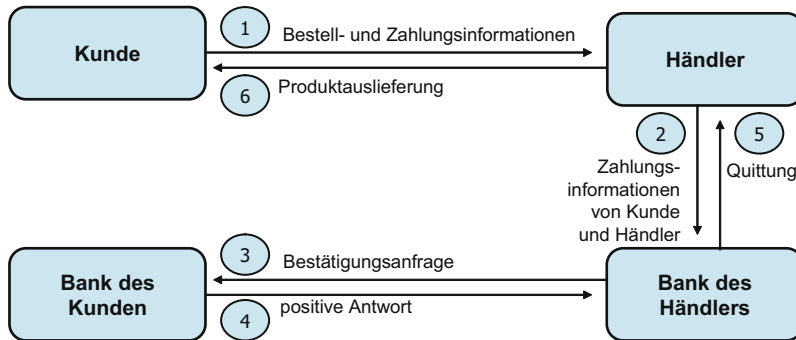


Abb. 7.3 Der Zahlungsprozess bei SET

- ▶ SET-Server für den Verkäufer
 - Der Verkäufer muss auf seinem Web-Server eine spezielle Software (SET-Server) installieren und betreiben. Der SET-Server kommuniziert sowohl mit dem SET-Wallet des Käufers als auch mit der Bank des Verkäufers.
- ▶ SET-Payment Server für die Bank
 - Die Banken von Käufern und Verkäufern müssen einen SET-Payment-Server bereitstellen.

SET ist eine kreditkartenbasierte Lösung. Will ein Käufer ein Produkt erwerben, gibt er seine Kreditkartennummer in sein SET-Wallet ein. Danach werden folgende Schritte ausgeführt (siehe Abb. 7.3):

- ▶ Beispiel einer SET-Transaktion
 1. Der Käufer schickt bei der Bestellung seine Zahlungsinformationen verschlüsselt und digital signiert an den Verkäufer.
 2. Der Verkäufer (bzw. sein SET-Server) unterschreibt die Zahlungsinformationen ebenfalls und leitet sie an seine Bank weiter.
 3. Dort werden die Daten vom SET-Payment-Server entschlüsselt und die digitalen Unterschriften kontrolliert. Sind die Daten korrekt, wird die Bank des Käufers zur Bestätigung angefragt.
 4. Antwortet die Bank des Käufers positiv, kann die Zahlung vollzogen werden.
 5. Als Bestätigung wird eine Quittung an den Verkäufer geschickt.
 6. Der Händler kann das Produkt an den Kunden ausliefern.

► Die duale Signatur von SET

Ein wichtiges SET-Verfahren ist die duale Signatur. Sie kommt in Schritt 1 zum Einsatz. Der Kunde erstellt dabei eine Nachricht an den Verkäufer (M_1) sowie an die Bank (M_2). In der Nachricht an den Verkäufer finden sich die Bestellinformationen, in der Nachricht an die Bank die Zahlungsinformationen. Beide Nachrichten werden mit den jeweiligen öffentlichen Schlüsseln (M_1 mit dem öffentlichen Schlüssel des Verkäufers ($K_{\text{pub,Verk.}}$), M_2 mit dem öffentlichen Schlüssel der Bank ($K_{\text{pub,Bank}}$)) verschlüsselt (PM_1, PM_2). Ausserdem wird aus beiden Nachrichten ein Hash-Wert errechnet (H_1 und H_2). Aus den beiden Hash-Werten erzeugt das SET-Wallet einen weiteren Hash-Wert (H_3). Dieser wird vom Käufer digital unterschrieben (SH_3). Die beiden verschlüsselten Nachrichten (PM_1, PM_2) werden zusammen mit dem unterschriebenen Hash-Wert (SH_3) an den Verkäufer geschickt. Dieser kann mit seinem privaten Schlüssel zwar die Bestellnachricht (PM_1) entschlüsseln (M_1 generieren), nicht jedoch die Zahlungsnachricht (PM_2) lesen. Aus der Bestellnachricht (M_1) erzeugt er einen Hash-Wert. Über den unterschriebenen Hash-Wert (SH_3) kann er die Korrektheit der Bestellnachricht überprüfen. Der Verkäufer unterschreibt anschliessend die vom Käufer verschlüsselte Zahlungsnachricht (PM_2) sowie den bereits vom Käufer unterschriebenen Hash-Wert (SH_3) und sendet alles zu seiner Bank. Diese überprüft zunächst die Signatur des Verkäufers, anschliessend entschlüsselt sie die Zahlungsnachricht (PM_2), berechnet einen Hash-Wert von dieser Nachricht, um zusammen mit dem unterschriebenen Hash-Wert (SH_3) die Korrektheit von (M_2) zu verifizieren. Ist alles in Ordnung, schickt sie die bereits erwähnten Quittungen und tätigt die Transaktion.

7.3 Guthabenbasierte Verfahren

Bei den guthabenbasierten Verfahren wird, im Gegensatz zur Kreditkarte, ein bestimmter Betrag im Voraus auf ein Konto geladen (Pre-Paid, siehe obige Klassifikation über den Zeitpunkt der Zahlung). Mit diesem Geld kann die Rechnung beglichen werden. Mit der Geldkarte wird zunächst eine regionale Lösung vorgestellt. Sie ist derzeit nur in Deutschland im Einsatz. Anschliessend erfolgt eine kurze Beschreibung der Paysafecard, die in Europa vertrieben wird und sich insbesondere für die Online-Zahlung eignet.

7.3.1 Geldkarte

Ein in Deutschland beliebtes guthabenbasiertes Verfahren ist die Geldkarte. Eine Änderung des Jugendschutzgesetzes verbietet seit 2007 den Verkauf von Zigaretten an Automaten mit Bargeld. Deshalb haben viele Hersteller ihre Automaten so umgerüstet, dass nur noch mit der Geldkarte bezahlt werden kann, da sie als Altersverifikation akzeptiert wird. Diese Gesetzesänderung hat der Geldkarte in den letzten Jahren viele neue Kunden beschert.

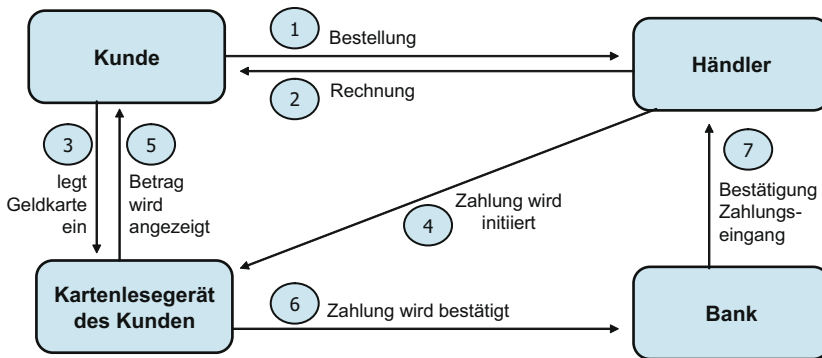


Abb. 7.4 Der Zahlungsprozess beim Online-Einkauf mit der Geldkarte

Die Geldkarte wird von Banken und Sparkassen ausgegeben. Maximal lassen sich bis zu 200 Euro auf einer Karte speichern. Das Geld kann auf verschiedene Arten, etwa über ein Terminal, spezielle Geldautomaten oder online auf die Karte geladen und anschliessend zum Bezahlen eingesetzt werden. Der Händler benötigt ein Terminal und eine Händlerkarte, mit der er sich authentifizieren kann.

► Geldkarte ist online einsetzbar

Die Geldkarte lässt sich im Online-Zahlungsverkehr nutzen. Der Kunde benötigt ein Kartenlesegerät, welches er an seinen Rechner anschliesst. Abbildung 7.4 illustriert den Online-Zahlungsprozess. Der Kunde sendet eine elektronische Bestellung an den Händler (Schritt 1) und erhält von diesem eine elektronische Rechnung (Schritt 2). Die Zahlung wird initiiert, indem der Kunde seine Geldkarte in das Kartenlesegerät einführt (Schritt 3), woraufhin sich Kunden- und Händlerkarte identifizieren (Schritt 4). Das Kartenlesegerät zeigt den Namen des Händlers, des Online-Shops sowie den zu bezahlenden Betrag (Schritt 5). Nach der Bestätigung durch den Kunden wird die Zahlung eingeleitet (Schritt 6). Der Händler bekommt eine Nachricht über die erfolgreiche Zahlung (Schritt 7) und kann das Produkt ausliefern.

► Geldkarte für inkrementelle Zahlungen

Neben der einmaligen Zahlung eines Betrags lässt sich mit der Geldkarte auch eine inkrementelle Zahlung durchführen. Wie bei einer Telefonkarte wird dabei ein kleiner Betrag zu einem bestimmten Zeitpunkt abgebucht. So lassen sich zahlungspflichtige zeitabhängige Online-Dienste realisieren.

Ein wichtiger Vorteil der Barzahlung ist die Anonymität des Käufers. Der Anbieter der Geldkarte betont, dass die Anonymität bei den angebotenen Lösungen garantiert bleibt. Allerdings ist es einfach, bei der Ausgabe der Karte den Empfänger abzuspeichern, was

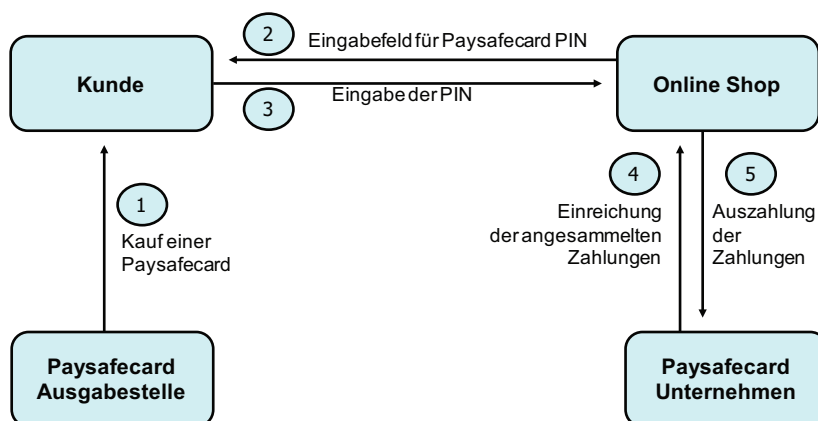


Abb. 7.5 Der Prozess beim Online-Einkauf mit einer Paysafecard.

aus steuerlichen Gründen teilweise erfolgt. Das Protokollieren der Käufe mit der Karte ist ebenfalls möglich.

Bei guthabenbasierten Verfahren ist die Sicherheit des Guthabens für die Anbieter von grösster Wichtigkeit. Gelingt es einem Angreifer, sein Guthaben auf der Karte abseits von einem Ladeterminal zu erhöhen, kann er beliebige Einkäufe tätigen. Diese Anforderung haben die Anbieter über die eingesetzten Smartkarten gelöst. Hier existieren mittlerweile sichere Verfahren.

7.3.2 Paysafecard

Die Paysafecard ist ein europaweit erhältliches guthabenbasiertes Zahlungsmittel mit Niederlassungen in vielen europäischen Ländern. Paysafecards können in herkömmlichen Verkaufsstellen, etwa Supermärkten oder Tankstellen, anonym erworben werden. Sie werden mit verschiedenen, bereits aufgeladenen Beträgen, verkauft. Die jeweiligen angebotenen Beträge unterscheiden sich von Land zu Land. Auch sind verschiedene Währungen möglich, in der Schweiz sind beispielsweise Karten in Schweizer Franken erhältlich, in Deutschland in Euro. Jede Karte besitzt einen eindeutigen 16-stelligen PIN-Code. Für die Bezahlung mit der Paysafecard wird lediglich dieser PIN-Code benötigt.

► Beispiel einer Paysafecard Transaktion

Abbildung 7.5 zeigt den Online-Einkauf mit einer Paysafecard. Ein Käufer muss zunächst eine Paysafecard an einer Ausgabestelle erwerben (Schritt 1). Anschliessend wird ihm, wenn er in einem Online-Shop mit dieser Karte zahlen möchte, ein Eingabefeld für den PIN-Code angezeigt (Schritt 2), welchen er zur Übermittlung an den Online-Shop

nutzen kann (Schritt 3). Sollte der Betrag grösser als der Restbetrag auf der Karte sein ist es möglich, mehrere PIN-Codes anzugeben. Es ist weiterhin möglich mit einer anderen Währung als der auf der Karte zu bezahlen. Der Betrag wird von Paysafecard automatisch umgerechnet. Der Online-Shop kann die Zahlung mit dem Code veranlassen (Schritt 4) und erhält den Betrag später vom Paysafecard.com Unternehmen ausbezahlt (Schritt 5).

Im Unterschied zur Geldkarte sind auf der Paysafecard keine Benutzerinformationen enthalten. Deshalb eignet sie sich nicht zur Altersverifikation, dafür ist sie anonym.

7.4 Innovative ePayment-Lösungen

Mitte der neunziger Jahre wurden viele ePayment-Lösungen vorgestellt. Obwohl sie konzeptionell interessant waren, konnten sie sich nicht am Markt durchsetzen. Im Folgenden werden einige dieser Ideen kurz erläutert.

7.4.1 eCash

- eCash arbeitet mit elektronischen Münzen

eCash ist eine Entwicklung der Firma DigiCash. Die Grundidee ist ein münzbasiertes System, welches die Vorteile von Bargeld in den elektronischen Zahlungsverkehr integriert. Bei eCash wird nicht zwischen Käufer und Händler unterschieden, jeder Benutzer besitzt die gleiche elektronische Geldbörse. In dieser werden „elektronische Münzen“ abgelegt. Führt der Benutzer eine Zahlung durch, werden Münzen aus der einen Geldbörse in die andere Geldbörse transferiert.

Beim Transfer elektronischer Münzen entstehen die gleichen Schwierigkeiten bezüglich Kopierschutz wie bei den guthabenbasierten Verfahren. Allerdings kommt bei eCash keine Smartkarte zum Einsatz, stattdessen verwendet eCash ein auf digitalen Signaturen basierendes Verfahren. Es wird von einer blinden Signatur gesprochen, um die Anonymität des Verfahrens zu betonen.

- Benutzer generiert eigene Münzen

Ein Benutzer von eCash generiert seine Münzen selbst und lässt sie von seiner Bank unterschreiben (siehe Abb. 7.6, Schritt 1 und 2). Akzeptiert die Bank die Münze, hebt sie den entsprechenden Betrag vom Konto des Benutzers ab. Die Münze ist ab diesem Zeitpunkt gültig. Eine Münze hat einen Wert (eine 2er Potenz von 0,01) und eine Seriennummer.

- Zufällige Seriennummer

Die elektronische Geldbörse des Benutzers generiert zufällig eine eindeutige Seriennummer. Diese wird verschlüsselt und mit den Zahlungsinformationen zur Bank gesendet.

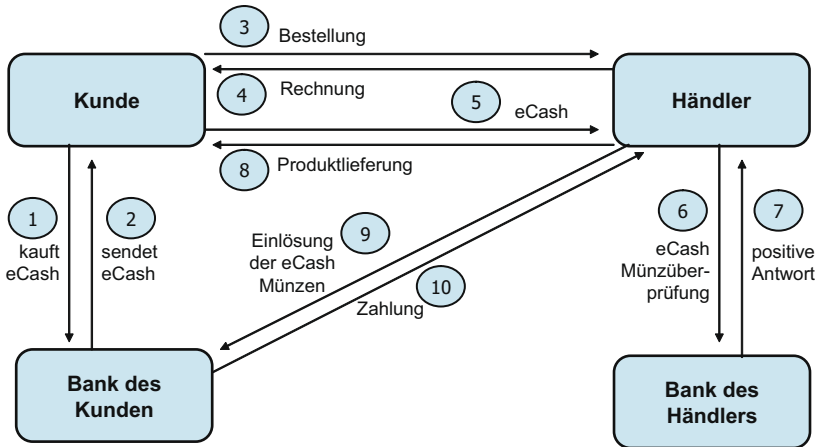


Abb. 7.6 Ablauf einer eCash Zahlung

Die Bank signiert die verschlüsselte Nummer. Für jeden Münzwert nutzt sie einen speziellen Unterschriftenschlüssel, über den bei der Bezahlung der Wert der Münze wieder erkannt werden kann. Neben Wert und Seriennummer werden in der elektronischen Münze noch eine Versionsnummer sowie ein Verfallsdatum gespeichert. Die signierte Münze wird zur elektronischen Geldbörse des Benutzers zurückgeschickt. Die Bank speichert in einer Datenbank jedoch, dass die Münze verteilt wurde. Der Benutzer entfernt die Verschlüsselung der Seriennummer.

► Beispiel einer eCash Transaktion

Möchte ein Kunde ein Produkt kaufen und mit eCash bezahlen (Schritt 3 und 4), sendet er seine Münzen an die elektronische Geldbörse des Händlers (Schritt 5). Von dort werden sie an den eCash-Server weitergereicht und man überprüft (Schritt 6), ob die Münzen bereits ausgegeben wurden. Sind die Münzen gültig (Schritt 7), kann der Händler das Produkt an den Kunden liefern (Schritt 8) und sich den Betrag auf sein Konto gutschreiben oder gegen neue Münzen austauschen lassen (Schritt 9 und 10).

► eCash mangelte es an Kundenakzeptanz

eCash wurde nach einer kurzen Testphase von den beteiligten Banken (Deutsche Bank, Mark Twain Bank USA, u. a.) verworfen, weil die Akzeptanz bei den Kunden fehlte. Ein Problem von eCash sind die Vorbedingungen, welche neben einer Anmeldung für den Service die Softwareinstallation für die elektronische Geldbörse umfassen. Ein weiteres Problem ist die komplexe Skalierung des eCash-Servers für die Überprüfung der Gültigkeit.

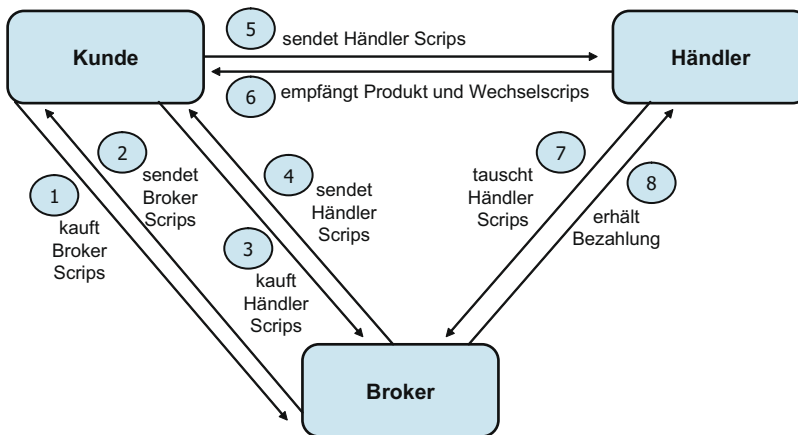


Abb. 7.7 Ablauf einer Millicent Zahlung

7.4.2 Millicent

- Millicent ist eine Art Inkassosystem

Die Firma Digital Equipment entwickelte die Millicent-Lösung, welche auf elektronischen Gutscheinen basiert. Millicent ist eine Art Inkassosystem, vergleichbar mit der Handhabung von Spielchips in Casinos. Wie der Name vermuten lässt, handelt es sich um eine Micro-/Picopayment-Lösung. Der Kunde kauft von einem Broker einen Chip, bei Millicent Scrip genannt. Mit diesem kauft er beim Händler ein. Der Händler sammelt die Chips und tauscht sie in grösseren Mengen beim Broker in Geld zurück.

- Reduzierung der Transaktionskosten

Ziel von Millicent ist die Reduzierung der Transaktionskosten, um Micropayment attraktiv zu machen. Die im Jahre 1998 durchgeführten Feldtests von Digital zeigten, dass Transaktionen mit 0,2 Cent noch profitabel sind. Heute ist Millicent allerdings nicht mehr verfügbar.

- Beispiel einer Millicent Transaktion

Um Millicent nutzen zu können, benötigt der Kunde eine virtuelle Geldbörse (Wallet). Diese sollte im Webbrowser integriert sein. Der Händler setzt auf dem Web-Server die Millicent-Software ein. Will der Kunde ein Produkt erwerben und mittels Millicent bezahlen, kauft er in einem ersten Schritt bei einem Broker entsprechende Broker Scrips (siehe Abb. 7.7, Schritt 1 und 2). Da der Bezug von Broker Scrips selten erfolgt, ist die Zahlung mit einer Macropayment-Lösung möglich.

- **Broker und Händler Scrips**

Jeder Srip besitzt eine eindeutige Seriennummer, so dass mehrfache Zahlungsversuche festgestellt werden. Bei der Zahlung muss ein Teil der Broker Scrips gegen Händler Scrips getauscht werden, was der Kunde ebenfalls beim Broker erledigt (Schritt 3 und 4). Mit den erhaltenen Händler Scrips bezahlt er das Produkt (Schritt 5). Der Händler liefert das Produkt (Schritt 6) und sammelt alle erhaltenen Händler Scrips, um sie periodisch beim Broker einzulösen (Schritt 7 und 8).

7.4.3 PayWord und MicroMint

- **PayWord basiert auf asymmetrischer Verschlüsselung**

Zwei weitere interessante Zahlungsverfahren stammen von Ronald L. Rivest und Adi Shamir. Das PayWord-Verfahren basiert auf der Berechnung von virtuellen Münzen und verlangt ein asymmetrisches Schlüsselpaar. Der Kunde richtet zunächst ein Konto bei einem Broker ein und erhält von diesem ein Zertifikat mit Kundennamen, Brokernamen, öffentlichem Schlüssel sowie weiteren Informationen. Mit dem Zertifikat überprüft der Händler, ob der Kunde PayWords erzeugen darf und diese vom Broker angenommen werden. Will der Kunde ein Produkt erwerben, erzeugt er die PayWords mittels einer Einweg-Hashfunktion (vgl. Abschn. 5.3.2). Er sendet den ersten berechneten Hashwert vor Beginn der Zahlung an den Händler. Will er eine Zahlung durchführen, berechnet er einfach die nachfolgenden Werte und sendet diese nach. Jeder berechnete Wert entspricht einer festgelegten Grösse, beispielsweise einem Cent. Der Händler überprüft die Zahlung durch den öffentlichen Schlüssel des Kunden und akzeptiert damit die Gültigkeit der virtuellen Münzen. Anschliessend wechselt er sie beim Broker.

- **Sicherheit von MicroMint durch teure Berechnungen**

Sollen keine asymmetrischen Schlüsselpaare für die Kunden eingesetzt werden, schlagen Rivest und Schamir das MicroMint-Verfahren vor. Bei diesem erstellt ein Broker die Münzen und verkauft sie an Kunden. Sie können nun zum Kauf genutzt werden, wobei der Händler die Gültigkeit der Münzen überprüft. Die Berechnung der Münzen ist teuer und verlangt gegebenenfalls spezielle Hardware.

7.4.4 Zufälliges Bezahlen

- **Ein Benutzer zahlt alles**

Ein ausgefallener Ansatz zur Bezahlung von Kleinstbeträgen stammt von Ronald L. Rivest. Er schlägt vor, nicht alle Benutzer für eine Transaktion zahlen zu lassen, sondern eine „Lotterie“ durchzuführen, bei der ein Benutzer zufällig ausgewählt wird. Dieser Benutzer

bezahlt die gesamten angefallenen Kosten. Auf diese Weise lassen sich die Transaktionskosten reduzieren. Gleichzeitig wird gemäss den Gesetzen der Stochastik jeder Benutzer zu einem Zeitpunkt mit grosser Wahrscheinlichkeit gezogen und muss die Kosten übernehmen.

7.5 Spezielle Lösungen für Online-Shopbetreiber

► Vertrauen für elektronische Zahlung aufbauen

Einige grosse Internet-Unternehmen haben in den vergangenen Jahren spezielle Lösungen für Online-Shopbetreiber entwickelt. Setzt ein Betreiber eine solche Lösung ein, kann ein Kunde, sofern er über ein Benutzerkonto bei dem entsprechenden Internet-Unternehmen verfügt, über dieses Konto die Zahlung veranlassen. Der Shopbetreiber erhält vom Internet-Unternehmen lediglich die Zahlung. In den meisten Fällen werden keine anderen Daten über den Kunden weitergegeben. Für Kunden ergibt sich bei einer solchen Lösung der Vorteil, dass sie dem grossen Internet-Unternehmen eventuell mehr Vertrauen als dem unbekannten Online-Shop entgegenbringen. Ausserdem sparen sie Zeit, weil die notwendigen Benutzerdaten nicht erneut eingegeben werden müssen.

Im Folgenden sollen zwei Verfahren aus diesem Bereich vorgestellt werden.

7.5.1 Google Checkout

► Lösungsvorschlag von Google

Das Google Checkout Interface wurde vom Unternehmen Google Inc. für die einfache Integration in vorhandene Online-Shops entwickelt. Derzeit steht es nur Händlern in den USA und Grossbritannien zur Verfügung. Es ist aber damit zu rechnen, dass der Dienst in naher Zukunft für weitere Länder geöffnet wird. Über ein einfaches API kann der Online-Shopbetreiber Google Checkout in seinen Shop integrieren. In einem ersten Schritt muss er ein Konto bei Google eröffnen. Dort erhält er eine eindeutige Identifikationsnummer, die so genannte Merchant-ID.

► Manuelles Verfahren

Für die Integration von Google Checkout in den Online Shop sind derzeit zwei unterschiedliche Verfahren implementiert. Beim ersten handelt es sich um ein manuelles Verfahren. Dem Shopbetreiber wird ein Interface für das manuelle Erfassen einer Bestellung bereitgestellt. Nach Abschluss der Erfassung wird eine eMail an den Kunden generiert, die die notwendigen Zahlungsinformationen bereitstellt. Der Kunde loggt sich mit seinen Google-Benutzerinformationen auf einer Google Checkout-Seite ein und bezahlt die Bestellung. Derzeit akzeptiert Google Checkout lediglich die Zahlung mit einer Kreditkarte,

allerdings könnten in der Zukunft weitere Zahlungsmöglichkeiten hinzugefügt werden. Nach der erfolgreichen Zahlung sendet Google eine Bestätigung via eMail an den Shopbetreiber, der die Bestellung abschliessen kann.

► Integratives Verfahren

Das zweite Verfahren bettet Google Checkout vollständig in den Online-Shop ein. Grundlage für die Integration ist eine Schnittstelle, die entweder auf HTML-Formularen oder XML-Dokumenten basiert. Der Betreiber kann entweder lediglich den Checkout-Prozess, also die Benutzeridentifikation, das Erfassen der Versand- und Zahlungsmethode sowie die Bestätigung an Google auslagern, oder aber alternativ bereits die Darstellung des Warenkorbs Google Checkout überlassen.

Fallbeispiel eDVDSHOP: Nutzung von Google Checkout im eDVDSHOP

Marcel Anderson möchte neben PayPal auch noch eine Google Checkout Anbindung in seinen Online-Shop integrieren. Dazu eröffnet er ein Konto bei Google und erhält seine Merchant-ID. Er entschliesst sich anschliessend für die Integrationsmethode über ein XML-Dokument, da sie mächtiger als die einfache Methode über HTML ist. Hierbei wird auf der Warenkorbübersichtsseite ein Google Checkout Button eingefügt. Ein Betätigen dieses Buttons erzeugt einen Request auf dem Server des Online-Shops. In diesem Request wird ein XML-Dokument erzeugt, welches die notwendigen Informationen bereitstellt, um die Bezahlung durchzuführen. Ein einfaches Beispiel sieht folgendermassen aus:

```
<?xml version="1.0" encoding="UTF-8"?>
<checkout-shopping-cart
  xmlns="http://checkout.google.com/schema/2">
  <shopping-cart>
    <items>
      <item>
        <item-name>DVD Blood Diamond</item-name>
        <item-description>Der Film Blood
          Diamond...</item-description>
        <unit-price currency="CHF">23.99</unit-price>
        <quantity>1</quantity>
      </item>
      <item>
        <item-name>DVD Babel</item-name>
        <item-description>Der Film
          Babel...</item-description>
        <unit-price currency="CHF">26.99</unit-price>
        <quantity>1</quantity>
      </item>
    </items>
  </shopping-cart>
  <checkout-flow-support>
    <merchant-checkout-flow-support>
      <shipping-methods>
```

```
<flat-rate-shipping name="Schweizer Post">
  <price currency="CHF">5</price>
</flat-rate-shipping>
</shipping-methods>
</merchant-checkout-flow-support>
</checkout-flow-support>
</checkout-shopping-cart>
```

Dieses XML-Dokument wurde durch die beiden Produkte „DVD Blood Diamond“ sowie „DVD Babel“, die sich im Warenkorb befunden haben, erzeugt. Der Online-Shop sendet das XML-Dokument an Google Checkout. Dort wird es empfangen und, im positiven Fall, eine URL zurückgesendet, auf die der Kunde die Bezahlung durchführen kann.

7.5.2 Amazon FPS

► Attraktives Angebot vom Amazon

Der Amazon Flexible Payment Service, kurz FPS, läuft über die Webseiten von Amazon. Amazon FPS geht im Unterschied zu Google Checkout viel weiter. So unterstützt FPS neben der Zahlung mit Kreditkarte alle anderen von Amazon erlaubten Zahlungsmethoden. Ausserdem erlaubt FPS die automatische Durchführung von wiederkehrenden Zahlungen oder die Durchführung von Zahlungen zwischen zwei anderen Personen, was etwa für die Realisierung von Marktplätzen notwendig ist. Interessant sind daneben die vielfältigen Methoden zur Annahme von Micropayment Beträgen. Diese lassen sich kombinieren, um Transaktionskosten zu sparen.

Die Kosten für Amazon FPS sind granular. Es werden sowohl die Zahlungsmethode, der Betrag als auch der Gesamtumsatz berücksichtigt. Eine Zahlung mit Kreditkarte für einen Betrag grösser als \$10 kostet 5 % des Betrags zuzüglich einer konstanten Gebühr von \$0,05.

7.6 Lösungen für kostenpflichtige Webseiten

Es existieren eine Reihe von Lösungen, die sich auf die Bezahlung kostenpflichtiger Webseiten spezialisiert haben. Im Folgenden werden einige von ihnen kurz vorgestellt.

7.6.1 Click & Buy

► Click & Buy benötigt eine Registrierung

Das Zahlungssystem Click & Buy bietet eine Lösung für kostenpflichtige Internetseiten. Es wird weltweit unterstützt, wobei die akzeptierten Zahlungsmethoden je nach Land va-

riieren. Um Click & Buy nutzen zu können, müssen sich sowohl Kunde als auch Anbieter anmelden. Beide Parteien müssen bei der Anmeldung ihre Zahlungsmethoden bekannt geben. Der Kunde kann die anfallenden Kosten per Kreditkarte oder in vielen Ländern über eine Abbuchung auf seinem Bankkonto begleichen. Der Anbieter erhält die eingegangenen Zahlungen normalerweise auf ein Konto ausbezahlt. Die Transaktionen werden gebündelt, wobei die Abrechnung monatlich erfolgt. Der Anbieter muss weiterhin die kostenpflichtigen Teile seiner Internetpräsenz bei Click & Buy registrieren und die Webseiten anpassen. Beim Besuch der Webseiten wird der Kunde über den Click & Buy Server geleitet und muss sich authentifizieren. Click & Buy stellt die Kosten dem Kunden in Rechnung und schreibt sie, abzüglich einer Gebühr, dem Anbieter gut.

Click & Buy bietet inzwischen eine Reihe von Diensten an. Neben kostenpflichtigen Webseiten lässt sich ein Zahlungssystem für kleinere Softwarelösungen, elektronisch abgelegte Berichte und Reports realisieren.

7.6.2 Allopass

- Bei Allopass wird über die Telefonrechnung bezahlt

Das von der französischen Firma Hi-Media angebotene Allopass-System ist eine weitere Micropayment-Lösung zur Bezahlung von Web-Inhalten. Beim Allopass-System wird über die Telefonrechnung bezahlt. Will der Kunde eine kostenpflichtige Seite betreten, wird eine Eingangsseite angezeigt, auf der sich ein Formular zur Eingabe eines PIN-Codes sowie eine Telefonnummer befinden. Ruft der Kunde bei der angezeigten Telefonnummer an, erfährt er dort den in das Formular einzutragenden PIN-Code. Nach der Eingabe wird die kostenpflichtige Seite angezeigt. Die Zahlung erfolgt über die Telefonrechnung.

Ein Vorteil von Allopass sind die geringen Voraussetzungen. Eine Anmeldung des Benutzers erübrigt sich, und es wird lediglich ein Telefon benötigt. Allopass ist anonym, da die Bezahlung nicht auf ein bestimmtes Telefon beschränkt ist und auch öffentliche Fernsprecher genutzt werden können. Nachteile sind die relativ grossen Aufwände für den Administrator des Webserver sowie der schlechte Ruf von kostenpflichtigen Telefondiensten.

7.6.3 Flattr

- Freiwilliges Bezahlen von Online Inhalten mit Flattr






Flattr ist ein Online Payment Dienst, der sich auf die Bezahlung von Webseiten und Blogs konzentriert. Im Unterschied zu den vorgestellten Lösungen setzt Flattr auf das freiwillige Bezahlen. Ein Blog oder Webseitenbetreiber kann einen Flattr Button unterhalb

eines Artikels platzieren. Jeder Leser hat dann die Möglichkeit, durch das Klicken auf diesen Button, dem Betreiber einen Betrag zuzuweisen. Voraussetzung ist, dass sich der Leser bei Flattr registriert, seine Zahlungsdaten hinterlegt und festlegt, wie hoch der monatlich zu spendende Betrag ist. Innerhalb eines Monats kann er anschliessend beliebig oft auf verschiedene Flattr Button klicken. Am Ende des Monats berechnet Flattr den auszuschüttenden Betrag für jeden Klick, indem der monatlich zu spendende Betrag durch die Anzahl Klicks geteilt wird, wobei Flattr eine prozentuale Gebühr (aktuell 10 Prozent) abzieht. Die Betreiber der angeklickten Buttons erhalten für jeden Klick diesen Betrag ausbezahlt.

7.7 Vergleich von ePayment-Lösungen

In Tab. 7.1 findet sich ein Vergleich der vorgestellten Lösungen PayPal, Geldkarte, Paysafecard, Google Checkout, Click & Buy sowie Allopas. Die Kosten variieren stark und sind für unterschiedliche Aufgaben ausgelegt. Die Anzahl der Nutzer zeigt die Dominanz von PayPal als eine der erfolgreichsten ePayment-Lösungen. Allerdings ist PayPal als Macropayment-Lösung nicht für alle Aufgaben geeignet.

Tab. 7.1 Vergleich von ePayment-Lösungen

	 Paypal	 Geldkarte	 Paysafecard	 Google Checkout	 Click & Buy	 Allopas
Anzahl Nutzer	Mehr als 140 Millionen	Mehr als 60 Millionen	Keine Angaben (mehr als 1000 Händler)	Keine Angaben (mehr als 500 Händler)	Keine Angaben (mehr als 7000 Händler)	Keine Angaben
Gebühren für den Verkäufer	1,9–3,9 % des Umsatzes + 0,35 €	0,3 % des Umsatzes (mind. 0,01 €)	5,5–19 % des Umsatzes	1,5 % des Umsatzes	49 € Anmeld. + 5 €/Monat + 7–35 % des Umsatzes	um die 30 % des Umsatzes
Nutzungsgebiet	Weltweit (aktuell 15 Währungen)	Deutschland	Europaweit (aktuell 5 Währungen)	USA und GB (für Kunden weltweit)	Mehr als 25 Länder weltweit	Westeuropa
Klassifizierung nach der Höhe des Betrags	Macro-payment	Micro-payment	Micro-payment	Macro-payment	Micro-payment/Picopayment	Micro-payment/Picopayment
Klassifizierung nach dem Zeitpunkt der Zahlung	Pay-Later	Pre-Paid	Pre-Paid	Pay-Later	Pay-Later	Pay-Later

► Kosten der Lösungen variieren stark

ePayment-Systeme wie Allopass oder Click & Buy konzentrieren sich auf kostenpflichtige Web-Angebote. Diese Micro/Picopayment-Lösungen versuchen die Transaktionskosten für einen Aufruf zu senken, so dass auch mit Kleinstbeträgen ein Gewinn erzielt werden kann. Gleichwohl sind die Kosten für den Nutzer im Vergleich zu PayPal von bis zu 30 % des Umsatzes bedeutend höher.

Die Geldkarte ist im Offline-Handel in Deutschland verbreitet, für den Online-Handel benötigt der Kunde jedoch ein Kartenlesegerät. Aus diesem Grund existieren bislang nur wenige Online-Händler, die die Karte akzeptieren. Im Unterschied dazu konzentriert sich Paysafecard auf den Online-Handel. Hier bietet die Lösung viele Vorteile und ist eines der wenigen ePayment-Varianten, mit denen eine anonyme Zahlung ermöglicht wird.

Dienste wie Google Checkout bieten Vorteile für Kunden und Online Shopbetreiber. Allerdings sind sie aus datenschutzrechtlichen Gründen umstritten.

7.8 Literaturhinweise

► ePayment wird in eBusiness Standardwerken behandelt

ePayment ist ein klassisches Thema des eBusiness. Deshalb behandeln die meisten Werke über eBusiness elektronische Zahlungsverfahren, wie bei Merz [120] oder Turban [187]. Einige Bücher setzen sich ausschliesslich mit dem Thema auseinander, wie Teichmann et al. [183], Dannenberg/Ulrich [36] oder Kou [99].

► Literatur zu PayPal

Informationen zum PayPal-Bezahlungssystem erhält man auf deren Homepage [130]. Dort findet sich auch eine Aufstellung der Kosten (siehe Tab. 7.1). Weiterhin existieren Dokumentationen zur Einbindung von PayPal in andere Systeme.

► SET ist standardisiert

Das SET-Protokoll wurde in drei Bänden veröffentlicht [165, 166, 167], die zusammen mehr als 1000 Seiten aufweisen. Im deutschsprachigen Bereich findet sich das Werk von Zwissler [202], welches den Standard kompakt aufbereitet. Es richtet sich dabei speziell an potenzielle SET-Anwender.

Die Geldkarte wird auf deren Homepage [56] genauer beschrieben. Interessierte Anbieter sowie Kartennutzer können sich auf dieser Seite registrieren. Gleiches gilt für die vorgestellte Paysafecard [131].

► Literatur zu innovativen Verfahren

Das eCash-Verfahren basiert auf zwei Arbeiten von Chaum [32, 33], die auf verschiedenen Fachkonferenzen veröffentlicht wurden. Von Schoenmakers stammt eine Arbeit über die Sicherheit von eCash [156]. Die vorgestellten theoretischen Verfahren PayWord, Micromint sowie zufälliges Bezahlen lassen sich in den Artikeln von Rivest und Shamir [143] bzw. Rivest [142] nachlesen.

Die vorgestellten Ansätze zur Bezahlung von kostenpflichtigen Webseiten können auf den Hompages der Anbieter Click & Buy [49], Hi-Media Allopass [8] und Flattr [50] genauer eingesehen werden.