

Paymentdienstleistungen für Online-Shops

1 Einleitung

Für alle Unternehmen, die wettbewerbsfähig bleiben möchten, ist e-Commerce als Vertriebskanal nicht mehr wegzudenken. Laut der International Data Corporation (IDC) werden im Jahr 2003 rund 250 Millionen Menschen über das Web Waren und Dienstleistungen umschlagen. Online-Käufer stellen hohe Ansprüche an die Lieferfähigkeit, eine kurze Lieferzeit und eine sichere Bezahlweise bei Bestellungen im Internet.

Entscheidend für den Erfolg von Electronic Commerce in einem derart verdichteten Logistik-System ist der Einsatz sicherer Zahlungssysteme. Die Mehrheit der Online-Shopper wünschen sich eine größere Sicherheit beim elektronischen Einkauf. Für drei von fünf, der von der britischen Marktforschungsgesellschaft Jupiter Communications¹ befragten Internet-Nutzer, ist die Unsicherheit im Umgang mit Kreditkarten-Informationen die entscheidende Hürde beim Online-Einkauf.

In diesem Beitrag werden ausgehend von klassischen Bezahlverfahren Paymentdienstleistungen für Online-Shops dargestellt. Diese werden aus Sicht des Kunden und Shopanbieters beleuchtet, um Entscheidungskriterien für die Auswahl eines Bezahlverfahrens im Dschungel der Anbieter zu geben.

2 Klassische Zahlungsverfahren

Unter klassischen Zahlungsverfahren sollen die Zahlungsmöglichkeiten verstanden werden, bei denen sich Kunde und Verkäufer noch face-to-face oder zumindest am Telefon gegenüberstehen. Die meisten Online-Verfahren sind letztendlich ein Transfer dieser Zahlungsmöglichkeiten aus der realen in die virtuelle Welt, so dass die meisten Risiken von Internet-Bezahlverfahren eine Erbe aus der realen Welt sind. Sie treten so massiv in Erscheinung, weil der mit der Globalisierung verloren gegangene direkte Kundenkontakt und der weltweite, verdeckte, illegale Zugriff auf Datenbestände von jedem Computer aus, in verstärktem Maße kriminelle Energien weckt.

Bei der Darstellung der klassischen Verfahren werden deshalb den Aspekten Vertraulichkeit und Authentifizierung besondere Aufmerksamkeit geschenkt. **Vertraulichkeit** meint: "Wie werden persönliche Zahlungsverkehrsdaten vor unberechtigtem Zugriff geschützt?" Unter **Authentifizierung** wird die Frage verstanden: "Wie weise ich mich als der rechtmäßige Besitzer des Zahlungsmittels aus?"

2.1 Rechnungsstellung (Überweisung) / Nachnahme

Die Bezahlung per Überweisung nach Rechnungsstellung ist das zur Zeit gängigste Verfahren. Der Kunde erhält eine Ware oder Dienstleistung und bezahlt diese durch eine Gutschrift auf das Konto des Händlers. Ist diese einmal getätigt, besteht keine Möglichkeit mehr diese ohne Einwilligung des Empfängers oder Nachweis einer Fehlbuchung wieder rückgängig zu machen. Ein vorher getätigter Kaufvertrag sichert dem Händler seinen rechtlichen Anspruch auf die Bezahlung. Existiert dieser nicht, z.B. bei einer telefonischen Bestellung bei einem Versandhaus, wird eine Bezahlung nach Rechnungsstellung nur dann angeboten, wenn ein gewisse Kundenbindung existiert, der Kunde z.B. schon mehrmals Ware bestellt hat und diese fristgemäß bezahlt wurde. Besteht diese Kundenbindung nicht, wird die Ware per Nachnahme zugestellt, d.h. der Kunde bezahlt beim Erhalt der Ware direkt an den Postboten. Bei der Bekanntheit des Verfahrens aus der realen Welt überrascht es nicht, dass es auch im Internet doppelt so oft eingesetzt wurde wie die Kreditkartenzahlung (Abbildung 1).

¹ 1. Quartal 2000

2.2 Kreditverfahren

Während das bargeldlose Bezahlen in den USA fast ausschließlich per Kreditkarte getätigt wird, besitzt in Deutschland nur jeder zehnte Erwachsene eine Kreditkarte. Ist dem Händler die Kreditkartennummer und das Ablaufdatum bekannt, kann er den gewünschten Betrag durch den Kartenherausgeber auf sein Konto verbuchen lassen. Dies geschieht in den meisten Fällen im Online-Verfahren, so dass der Händler direkt beim Kauf erfährt, ob die Karte gesperrt oder das Limit ausgeschöpft ist. Wenn der Kunde den Betrag nicht zahlen möchte, kann er unter Angabe von Gründen (häufig: Kartenmissbrauch durch Dritte) eine Rückbuchung anstoßen (charge-back). Der Händler hat in diesem Fall den finanziellen Schaden, den er durch Versenden und Rückfordern der Ware erleidet, zu tragen. Um dem Kartenmissbrauch vorzubeugen, authentifiziert sich der Kreditkartenhalter mit seiner Unterschrift und in manchen Fällen auch durch ein Passfoto auf seiner Kreditkarte. Dem Kunden werden die angefallenen Zahlungen zum Monatsende in Rechnung gestellt. Da die Kreditkartenunternehmen hier einen Kredit gewähren und auch die Transaktionskosten im Falle eines Charge-backs tragen, erklären sich die relativ hohen Servicegebühren (ca. 4%) die der Händler zu tragen hat.

2.3 Debitverfahren

Während der Kunde bei Kreditverfahren zum Monatsende seine Rechnung begleicht, wird bei Debitverfahren eine sofortige Abbuchung vom Konto getätigt. In Europa sind Debitkarten sehr gängig. In Deutschland besitzen ca. 90% der erwachsenen Bundesbürger eine Debitkarte wie z.B. die EC-Karte. Folgende Verfahren zur Zahlungsabwicklung werden in erster Linie angeboten:

- **Lastschriftinzug:** Bei diesem Verfahren liest der Händler die Bankverbindung des Kunden von der Karte ein und verwendet diese für eine Lastschriftbuchung vom Kundenkonto. Die Authentifizierung des Kunden erfolgt durch eine Unterschrift auf dem Buchungsbeleg. Trotzdem darf der Kunde die Buchung ohne Angabe von Gründen rückgängig machen. Der Händler steht dann in der Nachweispflicht einer Dienstleistung oder Warenauslieferung. Das Risiko liegt allein bei ihm, da die Banken keine Zahlungsgarantie geben. Trotzdem wird dieses Verfahren z.B. von Kaufhausketten gerne angeboten, da bis auf die geringe Buchungsgebühr keine weiteren Kosten entstehen. Dies wird sich aber in Zukunft ändern, da der Bankenverband an einer entsprechenden Verordnung arbeitet.
- **EC-Cash-Zahlung:** Hierbei authentifiziert sich der Kunde bei der Bezahlung mit einer persönlichen Identifikationsnummer (PIN). Die Zahlung ist hiermit autorisiert und die Abbuchung vom Konto des Kunden kann nicht widerrufen werden. Für diese Zahlungssicherheit wird der Händler mit einigen Gebühren zur Kasse gebeten, insbesondere wenn er nicht –wie z.B. die Tankstellenketten- über einen eigenen Netzbetrieb verfügt.
- **Maestro:** Diese Zahlungsmethode ist dem EC-Cash-Verfahren sehr ähnlich. Es findet seine Anwendung bei internationale Debitkarten und ermöglicht eine Autorisierung gegen ausländische Konten.

2.4 Bargeld

Zum Bezahlen mit Bargeld muss technisch nichts gesagt werden, da es jeder beinahe täglich nutzt. Das Augenmerk soll allerdings auf folgende Aspekte gelenkt werden:

- Bei der Übergabe von Bargeld fallen **keine Transaktionskosten** an.
- Es ist damit für Bezahlungen von **kleinen Geldbeträgen** geeignet. Es lohnt sich z.B. nicht am Kaugummiautomaten mit Kreditkarte zu zahlen, da die Gebühren höher wären als der Wert der Ware.

- Der Zahler bleibt **anonym**. Anhand des Geldscheins kann niemand erkennen, wer Zahlungen damit durchgeführt hat.
- Das Verfahren ist **einfach** anzuwenden. Selbst ein Kind ist in der Lage mit Bargeld zu bezahlen.

Im Internet hat sich bisher noch kein Verfahren etabliert, das alle o.g. Punkte erfüllt und damit bargeldähnlichen Charakter hat.

2.5 Prepaidverfahren

Bei diesen Verfahren entrichtet der Kunde im voraus einen Geldbetrag, der ihm auf ein meist kartengebundenes Konto gutgeschrieben wird. Die Telefonkarte der Telekom, die zum bargeldlosen Telefonieren in Telefonzellen eingesetzt wird, und die Prepaidkarten zum Aufladen von Handykonten sind Beispiele dafür. Eine allgemeingültigere Variante ist die **Geldkarte**, die bereits von einigen Banken in Form eines Mikrochips auf der EC-Karte herausgegeben wird. Diese kann mit einem Betrag bis zu DM 400,- an Geldautomaten aufgeladen werden und für Zahlungen z.B. an Fahrkartenautomaten oder Kassenautomaten im Parkhaus etc. eingesetzt werden.

3 Transfer der klassischen Verfahren in das Internet

Wie eine Befragung von Internet-Nutzern durch *Institut für Wirtschaftspolitik und Wirtschaftsforschung* der Uni Karlsruhe zeigt (Abbildung 1), werden in erster Linie klassische Bezahlverfahren im Internet eingesetzt.

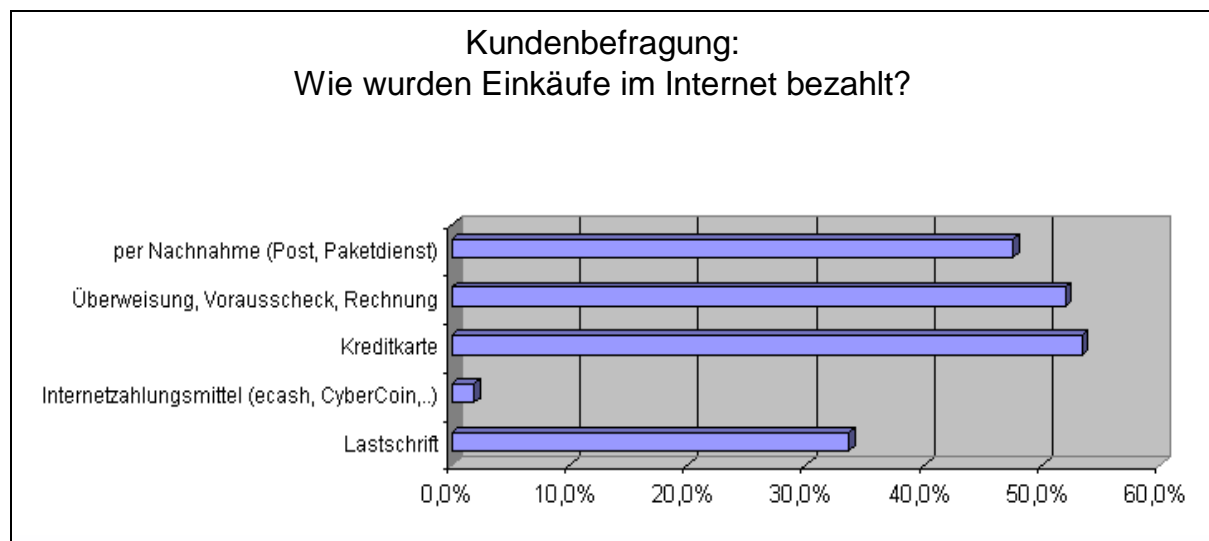


Abbildung 1: Bezahlverfahren im Internet (Stand: 1/2000)²

Ohne zusätzliche Sicherungsmaßnahmen werden damit die Nachteile aus der realen Welt übernommen und weitere hinzugefügt. Das größte Problem dabei ist die Anonymität der beiden am Handel beteiligten Parteien. Der Käufer kennt zwar den Rechner des Online-Shops aufgrund seiner (evtl. per SSL zertifizierten) Internetadresse, aber nicht den Shop-Betreiber, der hinter diesem Online-Shop steht. Gütesiegel und Prüfkriterien für Online-Shops versuchen hier Abhilfe zu schaffen und Mindeststandards zu garantieren.

² <http://www.iww.uni-karlsruhe.de:8001/IZV3/>



Abbildung 2: Gütesiegel für Online-Shops

Auf der anderen Seite kennt der Shop-Betreiber seinen (Erst-)Kunden überhaupt nicht und hat auch ohne zusätzliche organisatorische und technische Maßnahmen – die der Kunde unterstützen muss - keine Möglichkeit sicher herauszufinden, wer der Kunde ist. Er kann dementsprechend vom Kunden keine Unterschrift verlangen. Der Kunde kann nur über ein Bezahungsverfahren, z.B. über seine Kreditkartennummer und Gültigkeitsdatum, identifiziert werden. Statt sich also für die rechtmäßige Anwendung eines Bezahungsverfahrens zu legitimieren (z.B. Vorzeigen des Personalausweises zusammen mit der EC-Karte), identifiziert sich der Kunde über das Bezahungsverfahren. Das Verfahren kann dadurch leicht missbraucht werden. Um ein aus der realen Welt bekanntes Bezahungsverfahren für die Anwendung im Online-Bereich dennoch abzusichern, kann zu verschiedenen Hilfsmitteln gegriffen werden: Die Zahlungsverkehrsdaten (Kreditkartendaten, Bankverbindung etc.) können online auf Plausibilität geprüft, Sperr- und Blacklisten abgefragt und Adressinformationen validiert werden. Hinweise auf einen möglichen Missbrauch (z.B. IP-Adresse in Russland und Lieferadresse in Deutschland) können ausgewertet werden (Fraud-Protection). Letztendlich muss jedoch bei einem Missbrauch die geschädigte Partei die Beweislast tragen, da sie nicht die Möglichkeit hat, auf die Informationen einer rechtsverbindlichen Transaktion zurückzugreifen. Erst mit der Einführung einer rechtsverbindlichen Identitätsfeststellung kann die Beweislast umgekehrt werden. Im folgenden werden Sicherheitsmechanismen und Risiken der einzelnen Zahlungsverfahren im Internet dargestellt.

3.1 Rechnungsstellung

Die meisten privaten Internetnutzer benutzen eine Telefoneinwahl (ISDN oder analog), um eine Verbindung mit dem Internet herzustellen. Die entstehenden Telefonkosten erscheinen auf der monatlichen Telefonrechnung. Diese machen sich einige Anbieter zu nutze, indem sie Kosten für den Abruf von Webinformationen über die Telefonrechnung abrechnen. Dazu wird automatisch eine neue Einwahlverbindung über eine kostenpflichtige Telefonnummer hergestellt und so zeitgesteuert eine Transaktionsgebühr abgerechnet. Das bekannteste Verfahren ist NET900, das für Micropayment-Bezahlungen eingesetzt wird. Nachteil ist zur Zeit, dass diese Methode auf einer telefonischen Einwahl basiert und nicht für Festnetzverbindungen eingesetzt werden kann.

3.2 Kreditverfahren

Hierbei werden die Kreditkartendaten (Nummer und Ablaufdatum) vom Rechner des Kunden zum Händler-Server übertragen. Dies geschieht leider oftmals ohne jegliche Verschlüsselung der Verbindung. Kreditkartendaten können in diesem Fall sehr einfach abgehört und missbraucht werden. Abhilfe schafft hier eine SSL-verschlüsselte Verbindung (zu erkennen an dem Protokollzusatz **https**:). Dies sollte ein Mindeststandard sein, ohne den der Kunde seine Zahlungsdaten nicht preisgeben sollte. Da der Händler nicht feststellen kann, wer an dem gegenüberliegenden Rechner sitzt, bleibt trotzdem noch das große Risiko des Kartenmissbrauchs durch eine unbefugte Person. In diesem Fall muss der Händler mit einem charge-back rechnen.

Aus diesem Grund wird besonders von Händlerseite auf den Standard SET (secure electronic transaction) gesetzt. Dabei erhalten Kunde und Händler ein sog. Zertifikat, mit dem sie ihre Daten verschlüsseln und digital unterschreiben können. Der Kunde bezieht das Zertifikat bei seiner Bank und installiert es auf seinem Rechner mit Hilfe einer Wallet-Software. Diese startet automatisch immer dann, wenn eine Zahlung initiiert wird und kümmert sich um Verschlüsselung und die digitale Unterschrift. Auch der Händler ist auf eine Software zur Verwaltung seines Zertifikates und zur Abwicklung der Zahlung angewiesen. Diese hohen Investitionskosten von bis zu DM 25.000,- können gespart werden, wenn die Dienste eines Paymentproviders in Anspruch genommen werden, der gegen eine Transaktionsgebühr den Betrieb dieser Software übernimmt. Der große Vorteil von SET für den Händler ist, dass er vom Kreditkartenunternehmen eine Zahlungsgarantie erhält. Der Kunde hat den Vorteil, dass seine Zahlungsdaten so verschlüsselt werden, dass selbst der Payment-Provider und der Shop keinen Zugriff darauf haben. Erst der Kreditkartenprozessor kann diese sensiblen Daten entschlüsseln.

3.3 Debitverfahren

Für Debitverfahren gilt Ähnliches wie für Kreditkartenzahlungen. Auch hier bleibt das Risiko des nicht autorisierten Gebrauchs der Kontendaten. Da SET zur Zeit nur für Kreditkartenzahlungen implementiert wurde, werden hier andere Wege zur Sicherung beschritten. Einige Payment-Provider bieten Adressvalidierungs- und Scoringdienste an. Dabei wird vor der Zahlungsabwicklung die Lieferadresse und Anschrift überprüft und/oder eine Auskunft bei der Creditreform bzw. Schufa eingeholt. Eine echte Authentifizierung des Kunden ist dadurch allerdings nicht gegeben. Verfahren dazu werden im Kapitel 4.1 beschrieben.

3.4 Bargeld

Das einzige bargeldähnliche Internetbezahlverfahren ist eCash. Dabei erzeugt der Kunde auf seinem Rechner virtuelle Münzen, deren Echtheit er von einem Kreditinstitut zertifizieren lässt. Sein Konto wird mit dem entsprechenden Betrag belastet. Diese Münzen kann er zur anonymen Bezahlung im Internet verwenden. Der Shop reicht diese virtuellen Münzen bei der Bank ein und bekommt den entsprechenden Betrag gutgeschrieben. Die Verwaltung des virtuellen Geldes übernimmt auf Kundenseite eine Wallet-Software. Diese bietet bei einem Systemabsturz auch die Möglichkeit, die darin enthaltenen Münzen zu rekonstruieren. Da bei der Transaktion keine Gebühren anfallen, ist eCash auch für die Bezahlung von Kleinbeträgen (Micropayments) geeignet. Leider ist es zur Zeit wenig verbreitet und findet besonders auf Kundenseite wenig Akzeptanz.

3.5 Prepaidverfahren

Die **Geldkarte** kann auch zur Zahlung im Internet verwendet werden. Dazu benötigt der Kunde ein Kartenlesegerät, das ca. 100,- DM kostet. Dieses besitzt ein eigenes Tastenfeld und Display, um den Zahlungsbetrag direkt am Gerät zu bestätigen bzw. den genauen Empfänger überprüfen zu können. Dadurch wird verhindert, dass Viren auf dem Rechner Zugriff auf das virtuelle Geld der Geldkarte erhalten. Aufgrund des Hardwareaufwandes wird die Geldkarte im Internet zur Zeit wenig genutzt.

Die **paysafcard** ist eine Prepaid-Karte, die ähnlich wie eine Handy-Prepaidkarte eingesetzt wird. Der Kunde kauft eine Karte und kann den Gegenwert per Eingabe einer Seriennummer im Internet freischalten. Diesen Betrag kann er nach und nach in verschiedenen Shops ausgeben. Bei jeder Zahlung authentifiziert er sich durch erneute Eingabe der Seriennummer.



Abbildung 3: Geldkartenleser

Prepaidverfahren haben für den Händler den großen Vorteil, dass keine charge-backs zu erwarten sind. Außerdem eignen sie sich wegen der geringen Transaktionskosten besonders gut zur Abwicklung von Micropayments.

	Verfahren in der realen Welt	Umsetzung im Internet
Rechnung	Überweisung / Nachnahme	Inkassoverfahren (NET900 ³)
Kredit	Kreditkarte	Kartendaten mit SSL ⁴ , SET ⁵ verschlüsselt
Debit	EC-Karte, Lastschriftinzug, Maestro	Kartendaten mit SSL verschlüsselt oder via Dual-Channel (Paybox ⁶) authentifiziert
Bargeld	Münzen, Geldscheine	eCash ⁷
Prepaid	Telefonkarte, Prepaidkarte (Handy), Geldkarte	paysafecard ⁸ , Geldkarte ⁹

4 Sicht des Kunden

Beim Einkauf in Online-Shops kommt dem Aspekt der Spontanität eine große Bedeutung zu. Der Kunde erwartet eine schnelle Führung durch den Online-Shop, die exakt auf seine Bedürfnisse zugeschnitten ist. Das Bezahlssystem muss ebenfalls diesen Anforderung genügen. Der Shop-Betreiber kann i.a. nicht erwarten, dass der Kunde Vorbereitungen zur Nutzung eines bestimmten Bezahlverfahren getroffen hat (z.B. Installation eines Wallets). Der kleinste gemeinsame Nenner, auf den sich Händler und Kunde einigen sollten, ist der im Webbrowser des Kunden integrierte Standard (SSL, Cookies) sowie die aus der realen Welt bekannten Bezahlverfahren. Hauptanforderungen des Kunden sind dabei:

- einfache Anwendung
- Stornierungsmöglichkeit
- Vertraulichkeit der Daten

4.1 Einfache Anwendung

Die Verwendung der Kreditkarte bzw. des elektronischen Lastschriftinzuges ist bei der Verwendung im Online-Bereich unkompliziert. Es müssen lediglich die Zahlungsverkehrsdaten (Kreditkartennummer, Gültigkeitsdatum bzw. Kontonummer und Bankleitzahl) eingegeben werden. Diese Daten sollten ausschließlich über eine verschlüsselte Web-Verbindung (SSL) übertragen werden.

Der Kunde hat bei vielen Online-Shops die Möglichkeit sich mit seinen persönlichen Informationen registrieren zu lassen. Bei jedem weiteren Einkauf kann er dann mit einer Benutzerkennung und einem Kennwort auf seine Daten zurückgreifen. Die Möglichkeit von Falscheingaben aufgrund von Tippfehlern wird dabei minimiert. Zudem sind die vom Online-Shop gespeicherten Daten schon validiert. Für den Online-Shop bedeutet dies einen Vertrauensgewinn. Der Kunde kann sich auch bei einem Payment-Provider registrieren lassen. Zur Bezahlung identifiziert sich der Kunde gegenüber seinem Payment-Provider, der wiederum die Zahlung für den Online-Shop autorisiert. Der Kunde kann sich gegenüber dem Payment-Provider

³ <http://www.in-medias-res.com/products.htm>

⁴ http://www.weblogic.com/docs/classdocs/API_secure.html

⁵ <http://www.setco.org/>

⁶ <http://www.paybox.de/>

⁷ http://info4.deutsche-bank.de/global/ui/nav_ec.nsf/frameset/DMEL-47ULWU?OpenDocument

⁸ <http://www.paysafecard.com/>

⁹ <http://www.fun.de/deutsch/produkte/internetpayment/default.htm>

auf verschiedene Arten identifizieren. Im einfachsten Fall reicht eine Benutzerkennung und ein Kennwort. Ebenfalls kann eine smartcard-basierte Lösungen zum Einsatz kommen. In diesem Fall besitzt der Kunde einen Kartenleser und hat eine entsprechende Software seines Payment-Providers zum Auslesen des Kartenlesers installiert. Eine ähnliche, softwarebasierte Lösung ist der Einsatz von SSL-Client/X.509 Zertifikaten. Der Kunde hat in diesem Fall von seinem Payment-Provider ein Zertifikat erhalten und im Webbrowser installiert. Zur Bezahlung „schaltet“ der Kunde sein Zertifikat mittels Kennwort frei und autorisiert dadurch die Bezahlung. Eine gänzlich andere Möglichkeit der Authentisierung des Kunden wird bei sog. Dual-Channel Verfahren angewendet. Der Kunde macht im Online-Shop eine Angabe zu einem zusätzlichen „Authentisierungskanal“ (z.B. e-mail Adresse, Telefonnummer, Handynummer). Über diesen zusätzlichen Kanal erhält er eine Rückfrage, die er bestätigt. Damit wird dann die Bezahlung autorisiert. Das bekannteste Dual-Channel Verfahren ist Paybox. Dabei erhält der Kunde einen Rückruf auf seinem Handy. Durch die Antwort auf diesen Rückruf gibt er die Anweisung, die entsprechende Bezahlung gegenüber dem Online-Shop durchzuführen, d.h. er autorisiert die Zahlung

4.2 Stornierungsmöglichkeit

Der Kunde hat bei der Online-Bezahlung die gleichen Stornierungsmöglichkeiten wie bei der Bezahlung in der realen Welt. D.h. er kann bei Bezahlung mit einer Kreditkarte einen charge-back bzw. beim elektronischem Lastschriftzug eine Rückbuchung veranlassen. Der Händler muss eventuelle Forderungen untermauern (z.B. durch Nachweis der Versendung eines Artikels) und eigene Maßnahmen ergreifen um evtl. schon ausgelieferte Ware zurückzuerhalten.

Der Kunde kann nach dem neuen Fernabsatzgesetz innerhalb der gesetzlichen Frist die Ware zu Lasten des Händlers, ohne Angabe von Gründen, an diesen zurückschicken. Der Händler muss dem Kunden in diesem Fall die Kaufsumme zurückerstatten.

4.3 Vertraulichkeit

Bei der Bezahlung im Online-Shop besteht genau wie bei der Bezahlung in der realen Welt die Gefahr, dass die Zahlungsinformationen (Kreditkartendaten, Bankverbindungsdaten) durch Herausgabe in nicht vertrauenswürdige Hände gelangen bzw. illegal mitgeschnitten werden. In der Online-Welt ist das Mitschneiden von Information oft unbemerkt möglich, weshalb sich eine zusätzliche, verdeckte Gefahr ergibt. Hohe Vertraulichkeit bietet die Verwendung von verschlüsselten Verbindungen, z.B. SSL bei der Übertragung der Zahlungsverkehrsdaten. Höchste Vertraulichkeit ist gewährleistet, wenn die Zahlungsverkehrsdaten gar nicht übermittelt werden, sondern - wie oben beschrieben - vertraulich bei einem Payment-Provider hinterlegt sind.

5 Sicht des Shops

Die Auswahl eines geeigneten Zahlungssystems ist abhängig vom Angebot des Shops. Wird **Hardware** (z.B. Versandhäuser) ausgeliefert, sollte der Payment-Provider ein sog. Tracking der ausgelieferten Ware anbieten, d.h. er steht in Verbindung mit einem Zusteller (z.B. Deutsche Post, UPS) und vollzieht die Buchung erst nach Auslieferung der Ware. So werden unnötige und teure charge-backs vermieden und die Zufriedenheit des Kunden gewahrt. Als Zahlungssystem eignen sich daher besonders Debit- und Kreditverfahren. Viele Kreditkartenunternehmen unterstützen das Tracking durch eine mögliche Vorautorisierung eines Betrags zum Zeitpunkt des Kaufs und einem getrennten Verbuchen (capturing) nach Auslieferung der Ware.

Werden **virtuelle Waren** oder Dienste (z.B. Download oder Datenbankauskunft) angeboten, muss der Händler sicher gehen können, dass es zu keiner Stornierung durch den Kunden

kommt. Die Ware ist nach der Auslieferung über das Internet praktisch entwertet, da sie leicht kopiert werden kann. Eine Rückgabe macht in den meisten Fällen kein Sinn. Noch höhere Anforderungen muss der Händler stellen, wenn er virtuelle Waren im Wert von Kleinstbeträgen (**Micropayments**) anbietet. Beispiele hierfür sind Online-Magazine, die einzelne Artikel gegen Zahlung bereitstellen. Hier ist es im Falle einer Zahlungsstornierung gar nicht mehr möglich zu verfolgen, bei welchen Anbietern die kleinen Summen verbraucht wurden. Für diese Fälle sollten Prepaid- oder bargeldähnliche Verfahren eingesetzt werden.

5.1 Zahlungsgarantie

Kunde und Shopanbieter haben natürlich das gemeinsame Interesse Risiken zu vermeiden. Bezüglich der Sicherung des Kommunikationsweges lässt sich hier ein gemeinsamer Nenner finden. Bei der Frage nach dem Betrugsrisiko laufen die Anforderungen allerdings auseinander. Während der Shop Wert auf eine Zahlungsgarantie legt, hat der Kunde den Wunsch jederzeit zu stornieren. Debit- und Kreditzahlungen stellen hier eindeutig den Kunden besser, Prepaid-Lösungen bzw. bargeldähnliche Verfahren haben Vorteile für den Shopanbieter. Payment-Provider können hier als neutraler Dritter tätig werden. Gegen eine anteilige Gebühr bieten sie eine Zahlungsgarantie oder verwahren das Geld so lange auf einem Zwischenkonto bis beide Parteien das Geschäft komplett abgewickelt haben, der Kunde also seine Ware erhalten hat und damit zufrieden ist.

5.2 Einfache Implementierung

Bei der Entscheidung für eine Payment-Dienstleistung spielt gerade für kleinere Online-Anbieter der Implementierungsaufwand eine große Rolle. Es ist schwer abzuschätzen, ob nach einer großen Investition der break-even erreicht wird. Hier muss eine gutes Mittelmaß zwischen individueller Anpassung des Paymentsystems an den Shop und dem Implementierungsaufwand (ein Softwareentwicklungstag kostet bis zu DM 2500,-) gefunden werden.

5.2.1 Module für Standard-Shopsysteme

Betreibt der Anbieter ein Standard-Shopsystem (z.B. Intershop oder Openshop), so erhält er Module der verschiedenen Zahlungsanbieter, die er einfach integrieren kann. Diese Lösung ist einfach zu realisieren und in vielen Fällen ist das Zahlungsmodul kostenlos. Sie lässt natürlich wenig Raum für die individuelle Gestaltung der Zahlungsschnittstelle.

5.2.2 "Gehostete" Paymentlösungen

Bei dieser Variante bietet der Payment-Provider fertige Internetseiten zur Zahlungsabwicklung an, zu denen der Shopserver den Kunden umleitet (redirect). Dies macht besonders dann Sinn, wenn das Sammeln der Zahlungsinformationen sehr komplex sind. Als Beispiel ist die Abwicklung von europäischen Debitkarten zu nennen. Hier hat jedes Land ein eigenes Format der Bezahlenden, für das individuelle Eingabemasken bereitgestellt werden müssen.

Diese Variante erspart allerdings nicht den kompletten Programmieraufwand. Der Shop muss noch den Warenkorb auswerten und grundsätzliche Bezahlinformation (z.B. den Betrag) an den Payment-Provider übergeben. Der Aufwand hierfür ist aber sehr überschaubar und auf wenige Stunden zu begrenzen.

5.2.3 HTTP

Das HTTP-Protokoll ist das Standardprotokoll mit dem Daten zwischen Browser und Webserver übertragen werden. Es sieht nicht nur Befehle zum Abruf von Seiten vor (GET), sondern auch zum Übergeben von Parametern zum Webserver (POST). Diese Schnittstelle ist sehr einfach zu bedienen und wird von den meisten Payment-Providern angeboten. Sie ist unabhängig von der Wahl der Programmiersprache. Java, Java-Script, PHP, Perl und ASP sind

gleichermaßen geeignet. Da die Übertragung der Daten verschlüsselt mit SSL erfolgen sollte, ist es notwendig einen sog. SSL-Tunnel zu installieren. Diese Software steht als Freeware zur Verfügung. Ein erfahrener Webprogrammierer hat diese Schnittstelle innerhalb eines Tages erfolgreich realisiert und getestet.

5.2.4 Applet-Schnittstelle

Bei dieser Variante stellt der Payment-Provider ein JAVA-Applet zur Verfügung, das der Shop in seine Bezahlseite einbindet. Dieses Applet erfragt die Zahlungsdaten des Kunden und überträgt diese verschlüsselt zum Payment-Provider, ohne dass der Shop darauf Zugriff erhält. Aus Sicht aller Beteiligten ist dies eine sehr sichere Variante. Der Implementierungsaufwand für den Shop ist allerdings erheblich. Er muss für eine saubere Parameterübergabe seiner Shopdaten an das Applet sorgen und eine Schnittstelle bereitstellen, über die der Payment-Provider die Warenkorbdaten des Kunden abgleichen kann. Applets bereiten in seltenen Fällen Probleme im Browser des Kunden, falls dieser nicht die aktuelle JAVA-Version unterstützt oder ihre Ausführung aus Sicherheitsgründen deaktiviert wurde. Der Implementierungsaufwand ist mit zwei Tagen zu bemessen.

5.2.5 JAVA-Bibliothek

Viele Payment-Provider bieten zusätzlich zu ihrer HTTP-Schnittstelle eine JAVA-Klassenbibliothek an. Für den erfahrenen JAVA-Programmierer ist diese Anbindung sehr komfortabel, da auch komplexere Zahlungsverfahren wie z.B. SET gut unterstützt werden. Solche Bibliotheken verwenden implizit die SSL-Verschlüsselung oder eine äquivalente Methode.

6 Vorstellung einer Systemarchitektur

Eine mögliche Umsetzung o.g. Konzepte soll am Beispiel des Bezahlsystems des Payment-Providers ALLCASH Trust & Service International GmbH vorgestellt werden. ALLCASH bietet alle wichtigen Schnittstellen und Zahlungsmodule an und ermöglicht dem Online-Shop so eine hohe Flexibilität und die nötige Bandbreite, um auf einen möglichst großen Pool an potentiellen Kunden zurückgreifen zu können.

6.1 Shop-Schnittstellen

Das ALLCASH-System bietet folgende Schnittstellen zum Online-Shop:

- Die **JAVA-API** steht nur für SET-Zahlungen zur Verfügung und bietet komplexe Möglichkeiten zur Steuerung und Abfrage der Zahlungen. Um den Implementierungsaufwand klein zu halten, wurden die wichtigsten Befehle auch auf die HTTP-Schnittstelle abgebildet.
- **HTTP** ist die universellste Schnittstelle. Hierrüber können alle Bezahlwege inklusive der Adressvalidierung und des Scorings genutzt werden. Aufgrund der leichten Implementierung ist dies die meistgenutzte Variante.
- Das **Applet** kann für Kreditkartenzahlungen (ohne SET) und nationale Debitkarten verwendet werden. Adressvalidierung und Scoring werden dabei nicht angeboten.
- Die **Hostlösung** befindet sich zur Zeit in der Entwicklung und soll eine schnelle Anbindung besonders für europäische Debitkartenzahlungen ermöglichen.
- Darüberhinaus werden **Module** für gängige Shopsysteme angeboten, die allerdings nur die Standardzahlungsmethoden SSL-Kreditkartenzahlung und nationale Debitkarten umsetzen.
- In Zukunft wird auch eine Abrechnung von **Micropayments** angeboten. Diese wird in erster Linie auf das Modul für Prepaidkarten zurückgreifen.

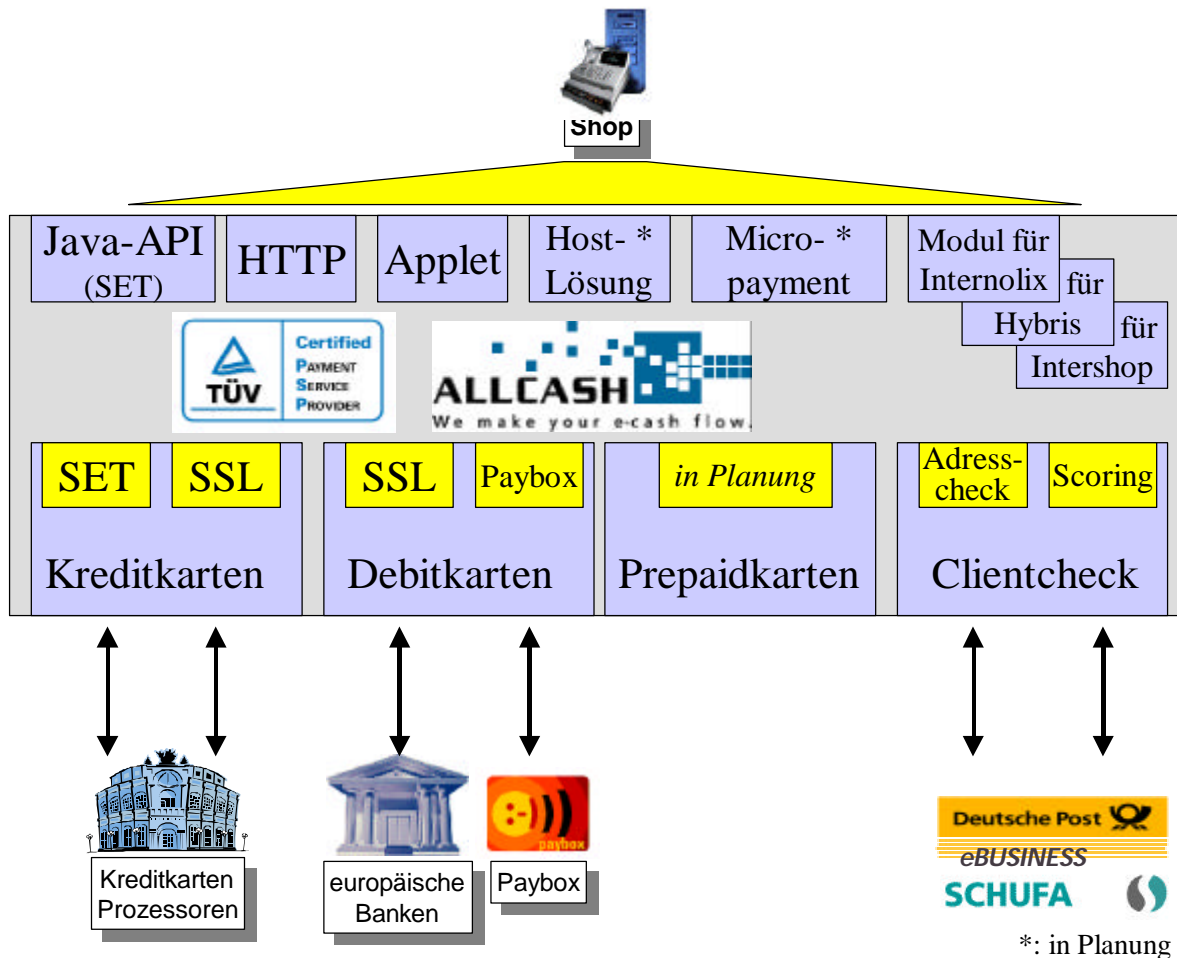


Abbildung 4: Struktur des Payment-Systems der Firma ALLCASH

6.2 Bezahlmodule

Im Bereich der Kreditkarten können SET- und SSL-Zahlungen abgewickelt werden. Debitzahlungen können zur Zeit nur national vollzogen werden. Im Jahr 2001 wird hier eine schrittweise Erweiterung für Zahlungen im europäischen Ausland durchgeführt. Zur Autorisierung der Debitzahlungen wird eine Schnittstelle zu Paybox angeboten. Ein Prepaid-Lösung wird zur Zeit entwickelt und soll insbesondere für Micropaymentzahlungen angeboten werden.

Um die hohe Anzahl der charge-backs zu minimieren und dem Missbrauch von Daten entgegen zu wirken, kann der Shop den Clientcheck durchführen lassen. Dieser ist ein mehrstufiger Prozess:

- **Adress-Check:** Die Anschrift wird einer Online-Prüfung unterzogen und der Händler erhält nur postalisch korrekte Adressen.
- **Identitäts-Check:** Dieser erlaubt Händlern auch die Überprüfung der postalischen Anschrift mit den Adresdaten (Vor- und Zuname) des Kunden.
- **Bonitäts-Check:** Die Ermittlung des Bonitätsstatus des Käufers erfolgt an Hand von Informationen aus dem öffentlichen Schuldnerverzeichnis und dem Inkassoverfahren des Versandhandels. Mit Hilfe der Bonitätsüberprüfung kann festgestellt werden, ob eine Person z. B. als säumiger Zahler bereits mehrfach aufgefallen ist, bzw. keine negativen Erkenntnisse über die Person vorliegen.

Autoren:

Matthias Lenord

Projektmanager eCommerce
ALLCASH GmbH
Eurotec-Ring 10
D-47445 Moers
*49-2841-1796-506
*49-2841-1796-521
lenord@allcash.de
www.allcash.de

Thomas Nisbach

Projektmanager eCommerce
ALLCASH GmbH
Eurotec-Ring 10
D-47445 Moers
*49-2841-1796-501
*49-2841-1796-521
nisbach@allcash.de
www.allcash.de