Wie werde ich mein Geld los?

Wie kommt der Händler an sein Geld?

Herausforderungen

- Händler kennt den Kunden meist nicht.
- Es gibt sehr viele verschiedene Zahlungssysteme, aber nur wenige sind weit verbreitet.
- Man muss zwischen b2c und b2b unterscheiden.
- Nicht jedes Zahlungssystem ist für jeden Kauf geeignet.
- kein Zug-um-Zug-Geschäft
- Internet ist eine Form des Versandhandels, doch viele Händler haben keine Erfahrung damit.
- Das Risiko für die Händler muss minimiert werden, da idR sie die Leidtragenden sind.

Entwicklung des elektronischen Geldes

Weg vom Bargeld

- Girokonto/Überweisungen
- Homebanking (Telefon, Internet)

Debitkarte (z.B. ec-Karte)

- enthält BLZ und Kontonummer
- speichert kein Geld
- Zahlung/Abhebung mit PIN (online-Authentifikation)
- Zahlung mit Unterschrift (vereinfachtes Lastschriftverfahren, Widerrufsmöglichkeit)

Entwicklung des elektronischen Geldes

Kreditkarte

- Zahlung mit Unterschrift
- verzögerte Zahlung

Geldkarte

- speichert Geld
- Zahlung ohne Autentifizierung

Vorteile von Bargeld

- begrenztes Verlustrisiko
- gebührenfreie Transaktion
- spurlos
- weitgehend anonym
- peer-to-peer Transaktion möglich

Kategorisierung der Bezahlsysteme

Pre-Paid-Systeme

Hardwarebasiert
z.B. Geldkarte
Softwarebasiert
z.B. CyberCoins, eCash

Pay-Now-Systeme

Nachnahme (offline)
Paybox

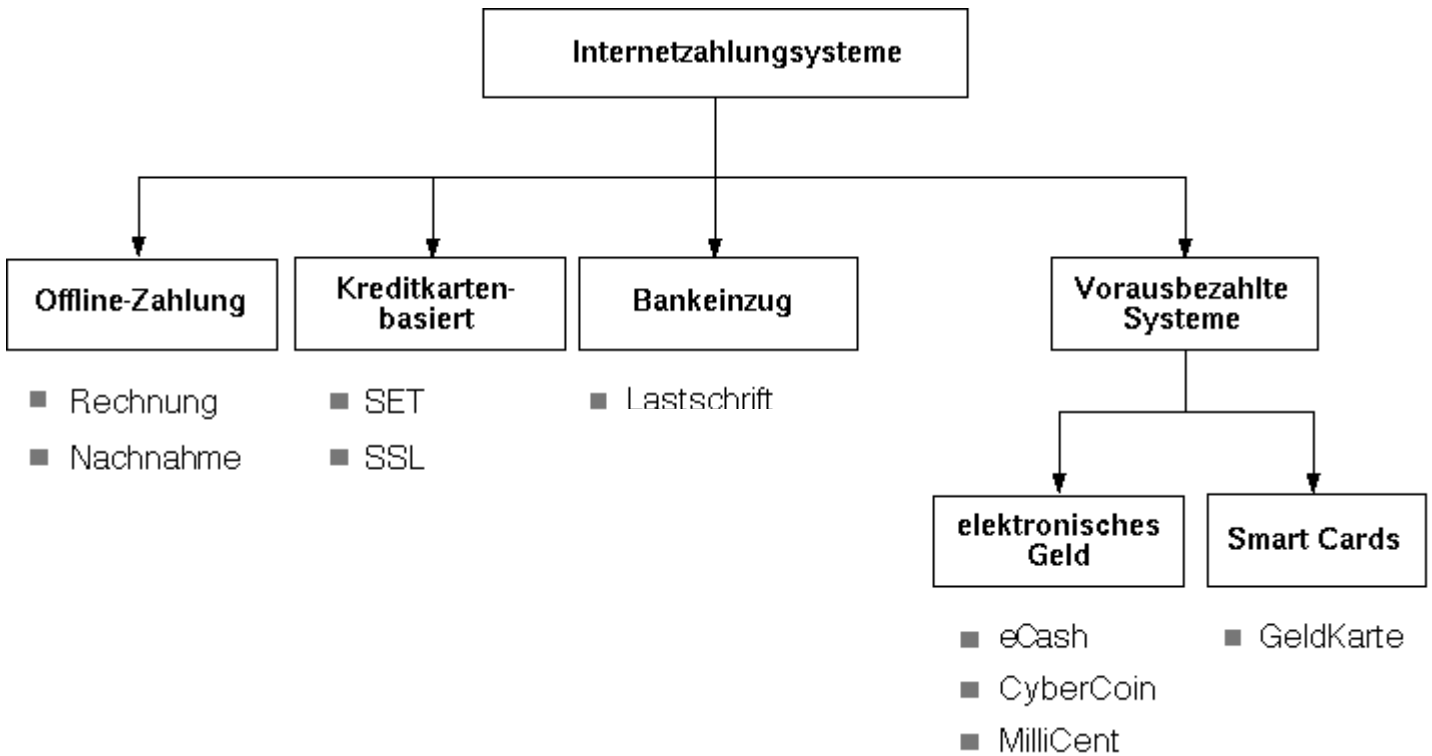
Pay-Later-Systeme

Kreditkartenbasiert
Ungesichert
SSL
SET (Varianten)

Inkaso/Billing
Net900
Firstgate Click&buy

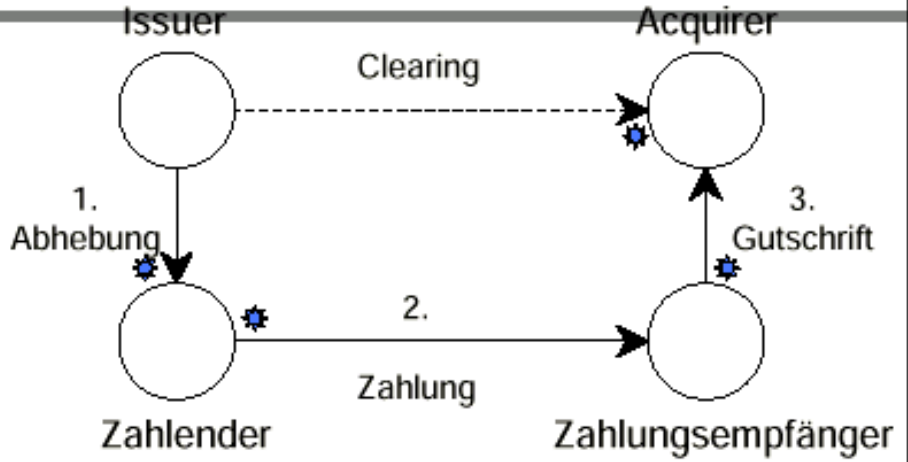
Rechnung
Überweisung
Lastschrift

Kategorisierung der Bezahlsysteme



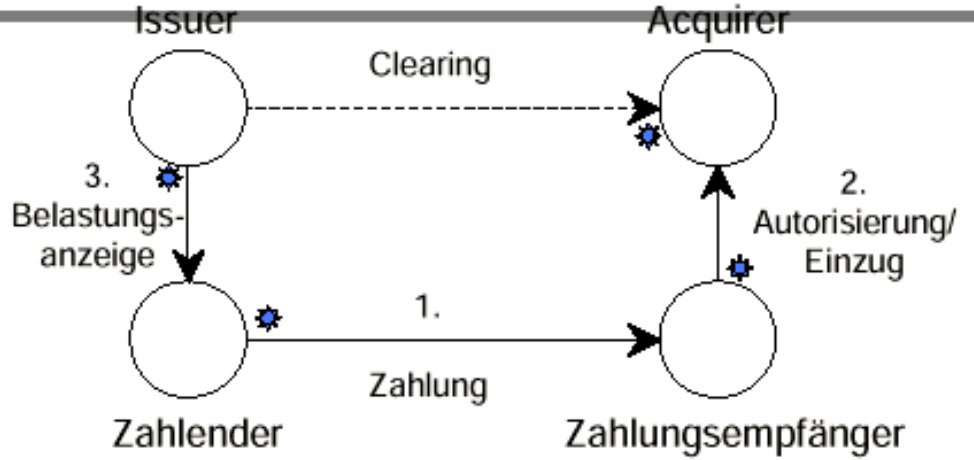
„Cash-like"-Zahlungssysteme (**online**)

Beispiel: eCash, Mondex, Geldkarte



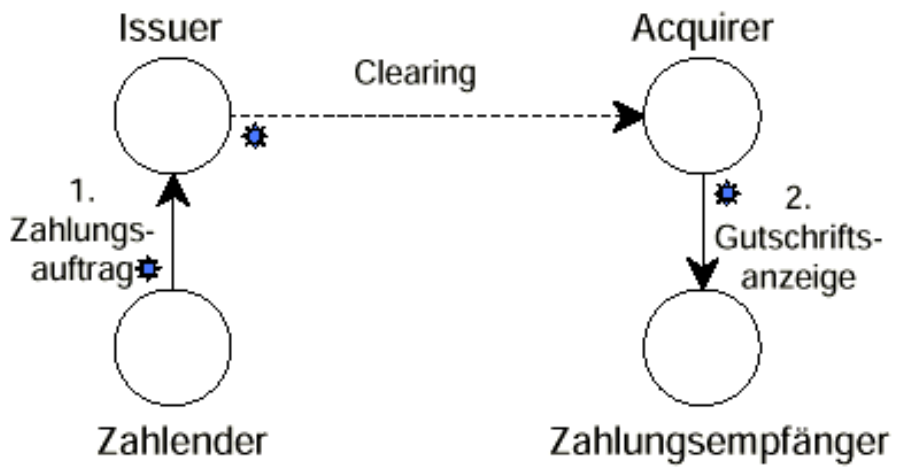
„Cheque-like"-Zahlungssysteme (**online**)

Beispiel: Kreditkarte SET/SSL, Internet-to-paybox



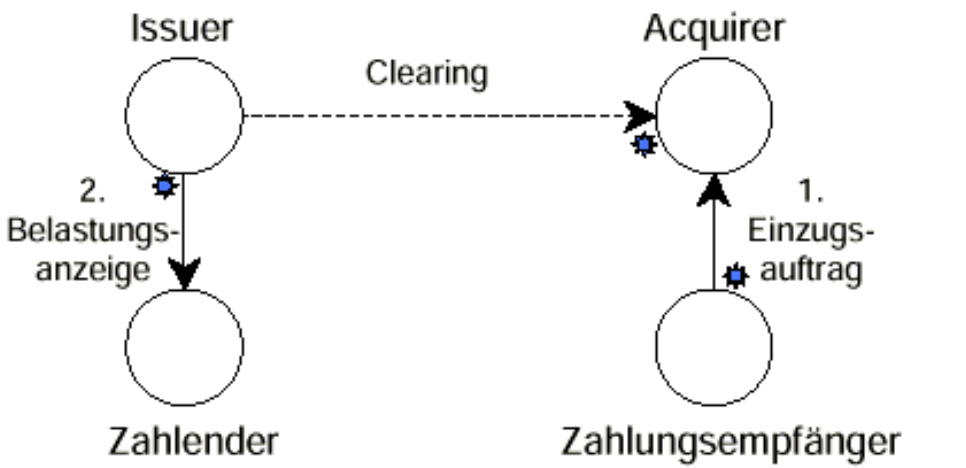
„Push-like"-Zahlungssysteme (**offline**)

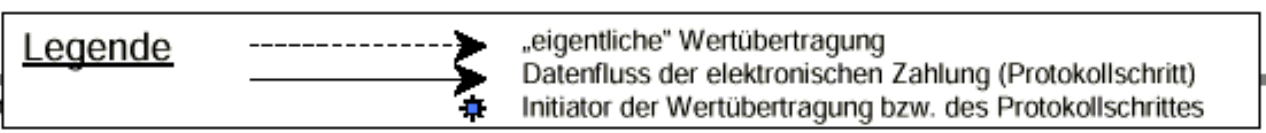
Beispiel: Online-Überweisung (HBCI)



„Pull-like"-Zahlungssysteme (**offline**)

Beispiel: Elektronische Lastschriftverfahren





Quelle: Institut für Informatik und Gesellschaft, Uni Freiburg

Online-Umfrage IZV

- IZV Internet-Zahlungssysteme aus Sicht der Verbraucher
- Institut für Wirtschaftspolitik und Wirtschaftsforschung - Universität Karlsruhe (TH) - Sektion Geld und Währung http://www.iww.uni-karlsruhe.de
- 7139 Teilnehmer
- nicht repräsentativ

Teilnehmer-Profil

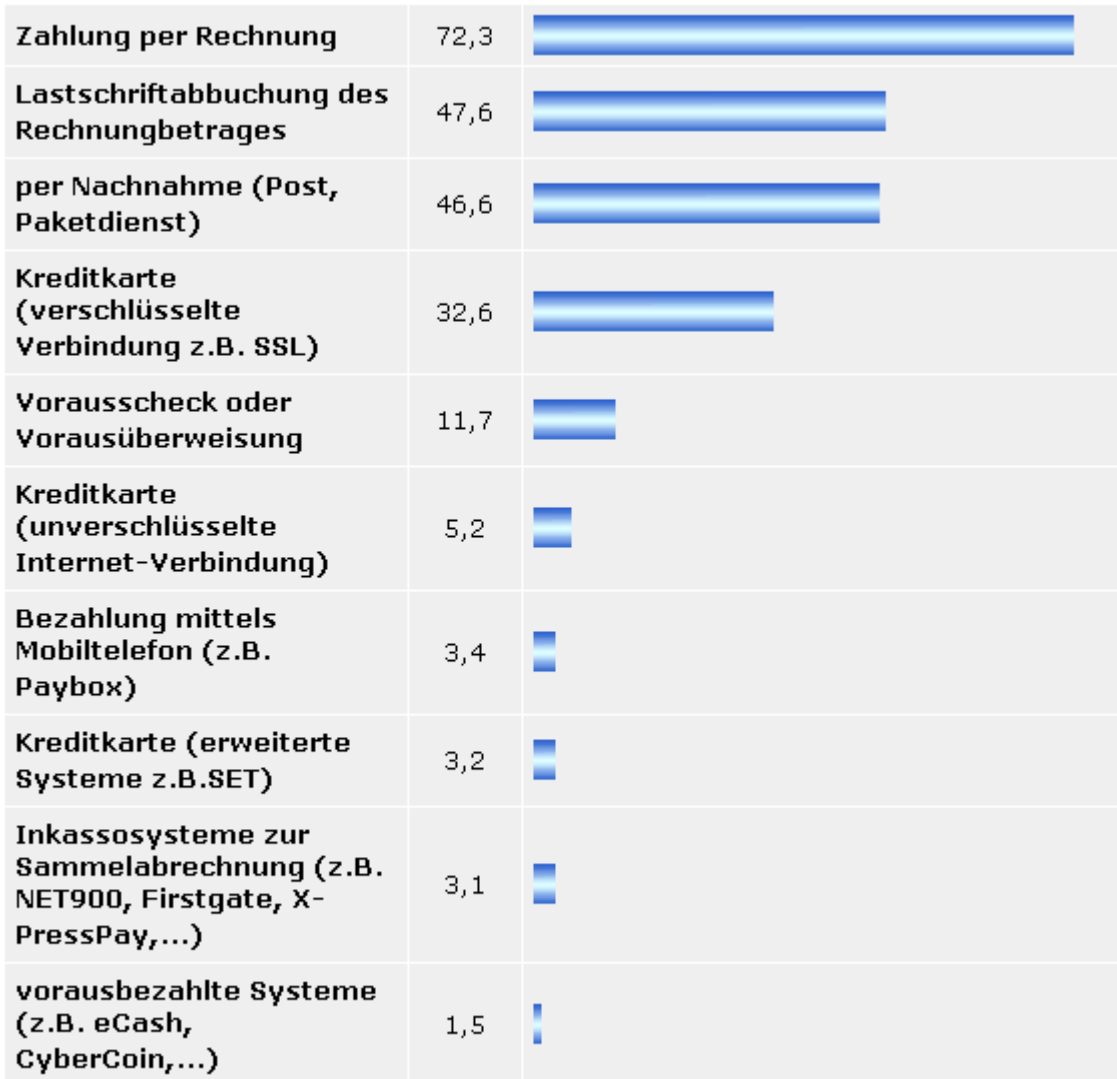
- 28,5% Frauen
- Intensive Internetnutzer
- 9 von 10 haben schon im Internet eingekauft
- 50% Kreditkartenbesitzer

Fragen

- Internetnutzung
- Wahl der Bezahl-Methode
- Rechtssicherheit/Digitale Signaturen, Micropayment
- Einsatz guthabenbasierter Systeme
- Wertung Erfahrungen Online-Shopping
- Hemmnisse Online-Shopping
- Einkaufen im Internet – Wünsche
- Personendaten

Bisher bevorzugte Bezahlmethoden

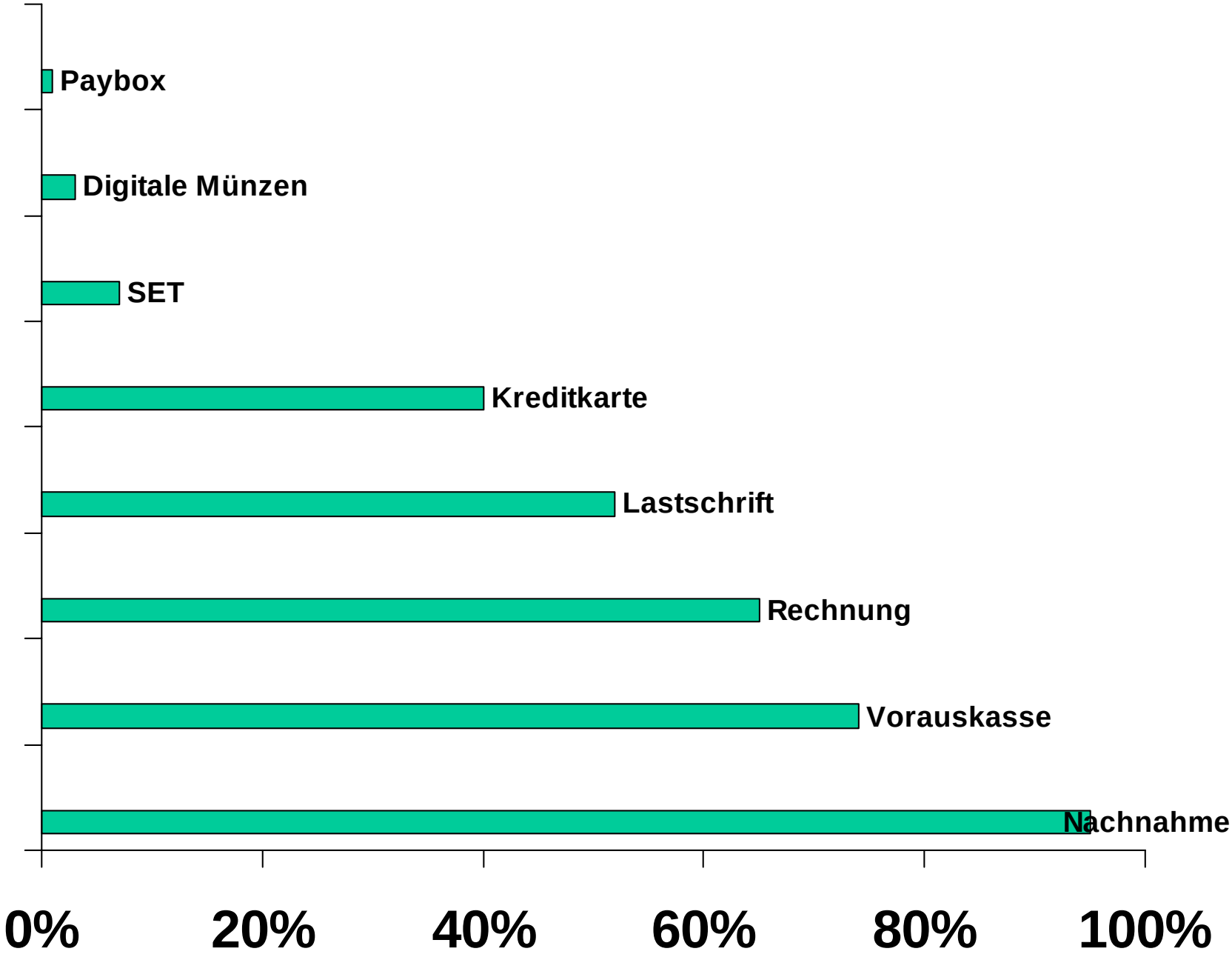
Angaben in %



Zahlung per Rechnung	72,3
Lastschriftabbuchung des Rechnungbetrages	47,6
per Nachnahme (Post, Paketdienst)	46,6
Kreditkarte (verschlüsselte Verbindung z.B. SSL)	32,6
Vorausscheck oder Vorausüberweisung	11,7
Kreditkarte (unverschlüsselte Internet-Verbindung)	5,2
Bezahlung mittels Mobiltelefon (z.B. Paybox)	3,4
Kreditkarte (erweiterte Systeme z.B.SET)	3,2
Inkassosysteme zur Sammelabrechnung (z.B. NET900, Firstgate, X-PressPay,...)	3,1
vorausbezahlte Systeme (z.B. eCash, CyberCoin,...)	1,5

Mehrfachnennungen möglich

Angebotene Bezahlsysteme kleinerer Shops



Quelle: Berelcon Research 2001

Probleme der beliebten Zahlungsmittel

Rechnung

keine Zahlungssicherheit, verspätete Zahlungen

Lastschrift

Kunden: Sicherheitsrisiko bei Datenübertragung, Möglichkeit von Fehlbuchungen, Voraussetzung Girokonto

Händler: ungewisse Deckung des Kontos, kein internationales Zahlungsmittel

Probleme der beliebten Zahlungsmittel

Kreditkarte

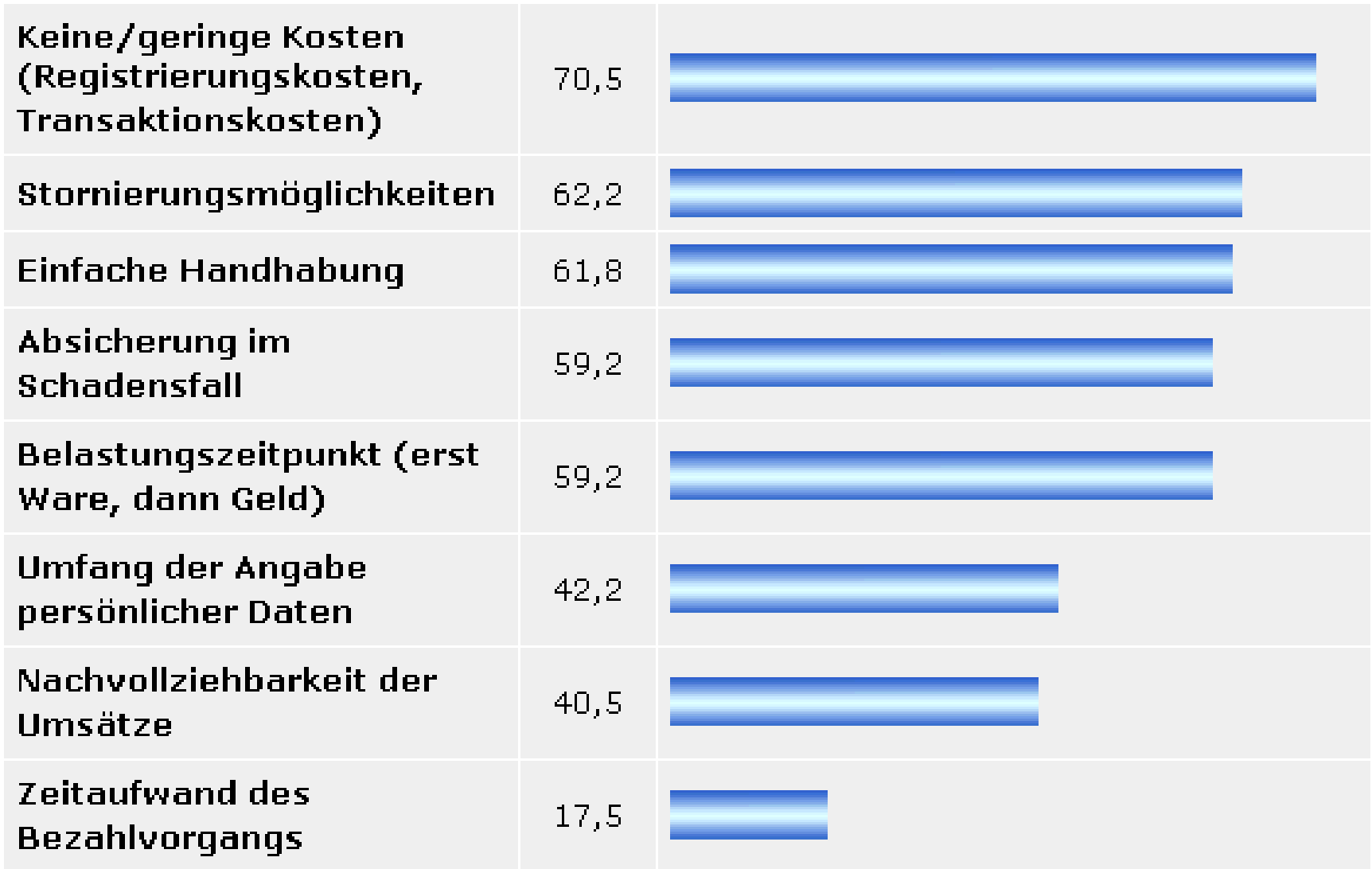
Kunden: Sicherheitsrisiko bei Datenübertragung, Möglichkeit von Fehlbuchungen, Voraussetzung Kreditkarte
Händler: relativ hohe Provision an Kreditkartenunternehmen, keine Gewissheit über Kunden

Nachnahme

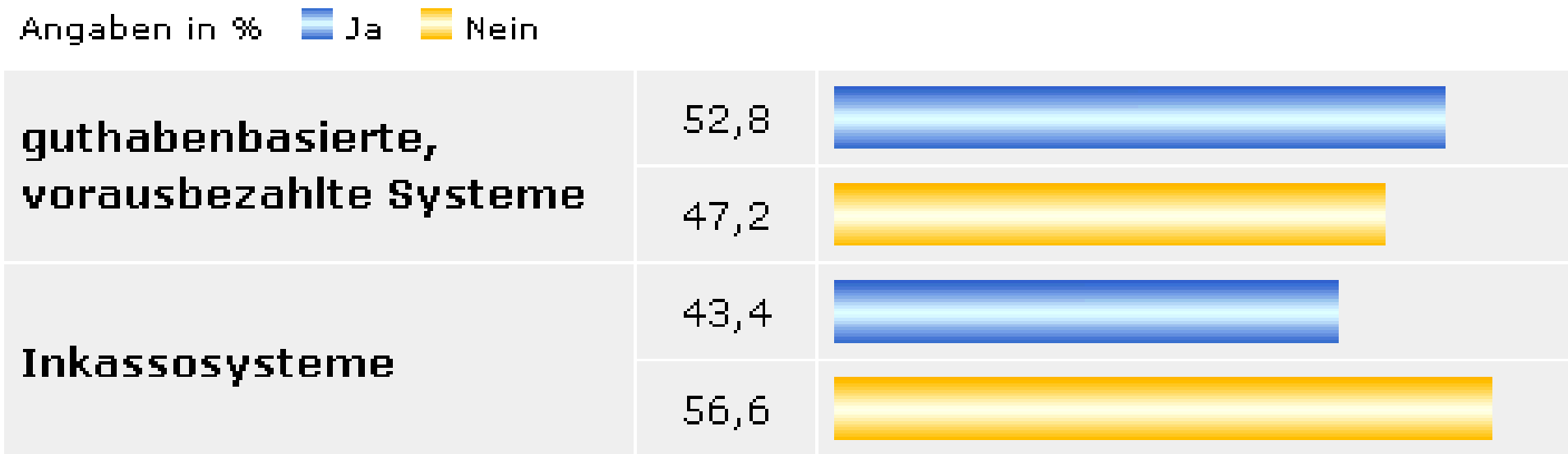
Kunden: Nachnahmegebühr, Kunde muss entweder zuhause sein oder zur Post gehen
Händler: aufwendige Übernahme der Daten ins Buchungssystem

Welche vier Kriterien sind Ihnen bei der Wahl des Zahlungsmittels am wichtigsten?

Angaben in %

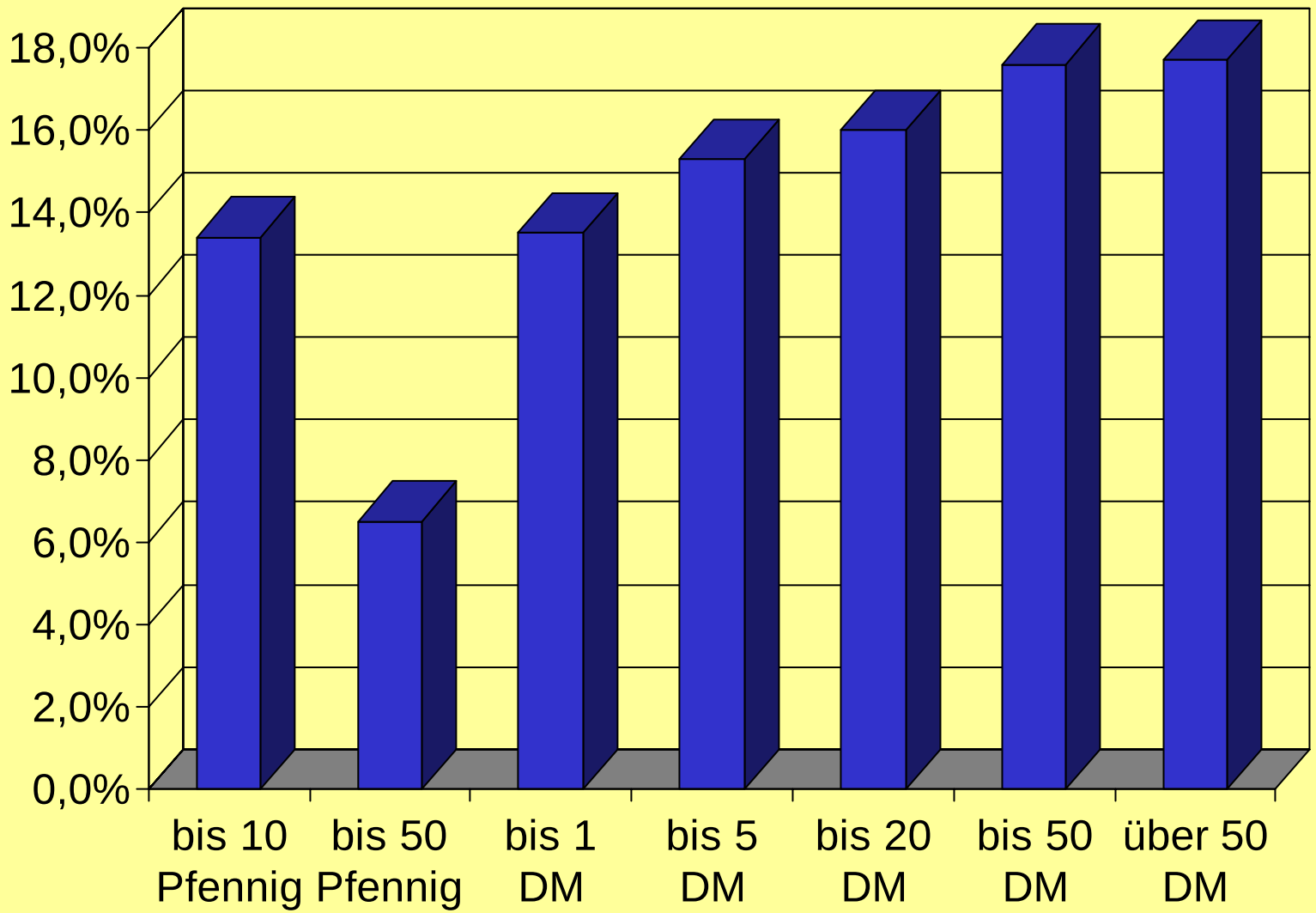


Innovative Bezahlverfahren



-

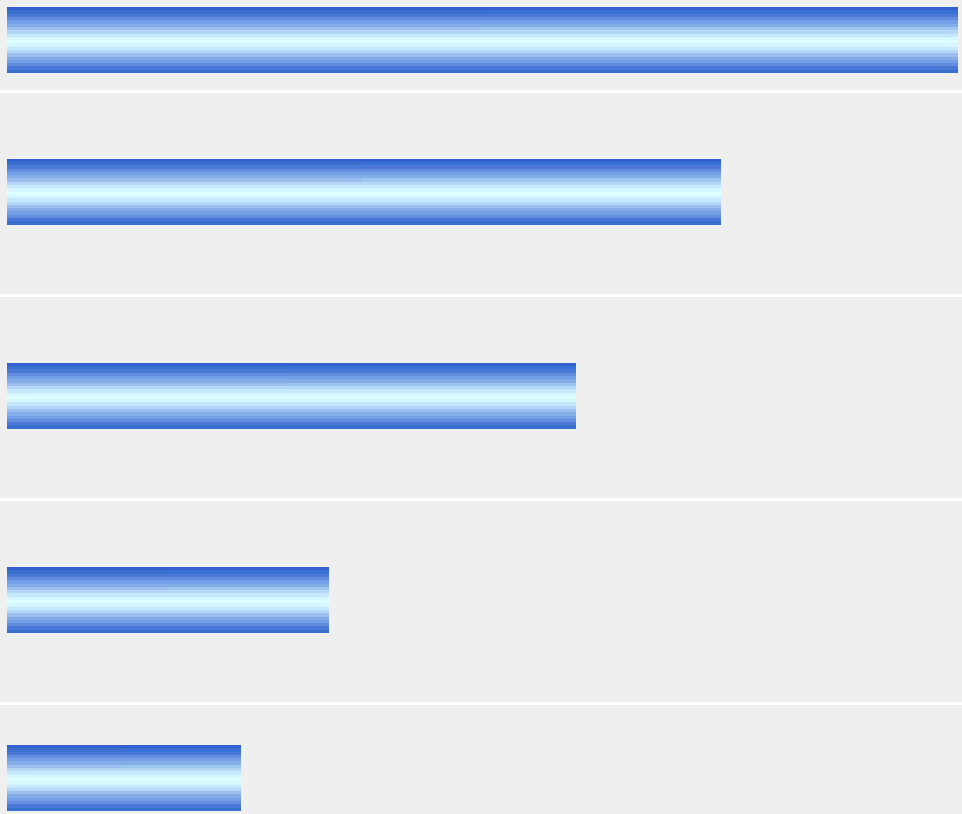
Maximaler Betrag pro Click bei Bezahlen mit Pay per Click



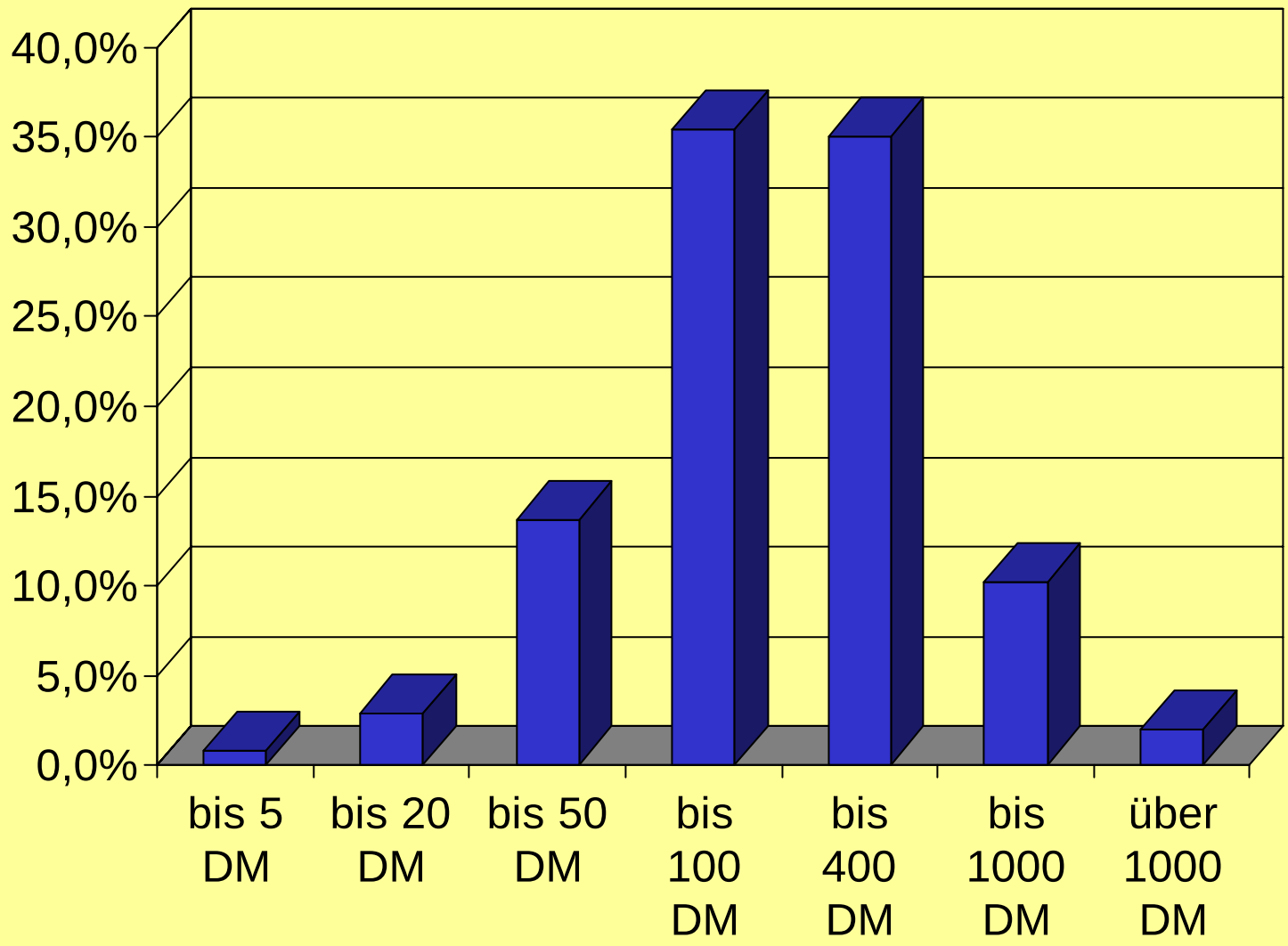
Bevorzugte Inkassounternehmen

Angaben in %

Banken	77,7
Kreditkarten-Unternehmen (z.B. Visa, Eurocard, MasterCard)	58,9
Telekommunikations-Unternehmen (z.B. Deutsche Telekom)	46,1
Internet-Service-Provider (z.B. AOL, T-Online, AddCom)	26,9
unabhängige Dritte (z.B. Firstgate click&buy)	19,4



Maximaler Betrag in elektronischer Geldbörse



Gründe für die Ablehnung von Inkassosystemen

- Mangelnde Budgetkontrolle (53,1%)
- Fehlendes Vertrauen in die technische Abwicklung (44,8%)
- Intransparenz des Verfahrens (40,5%)
- Unbekanntes System (29,6%)
- Zu aufwendig (20,6%)
- Kein Zusatznutzen ersichtlich (18,9%)

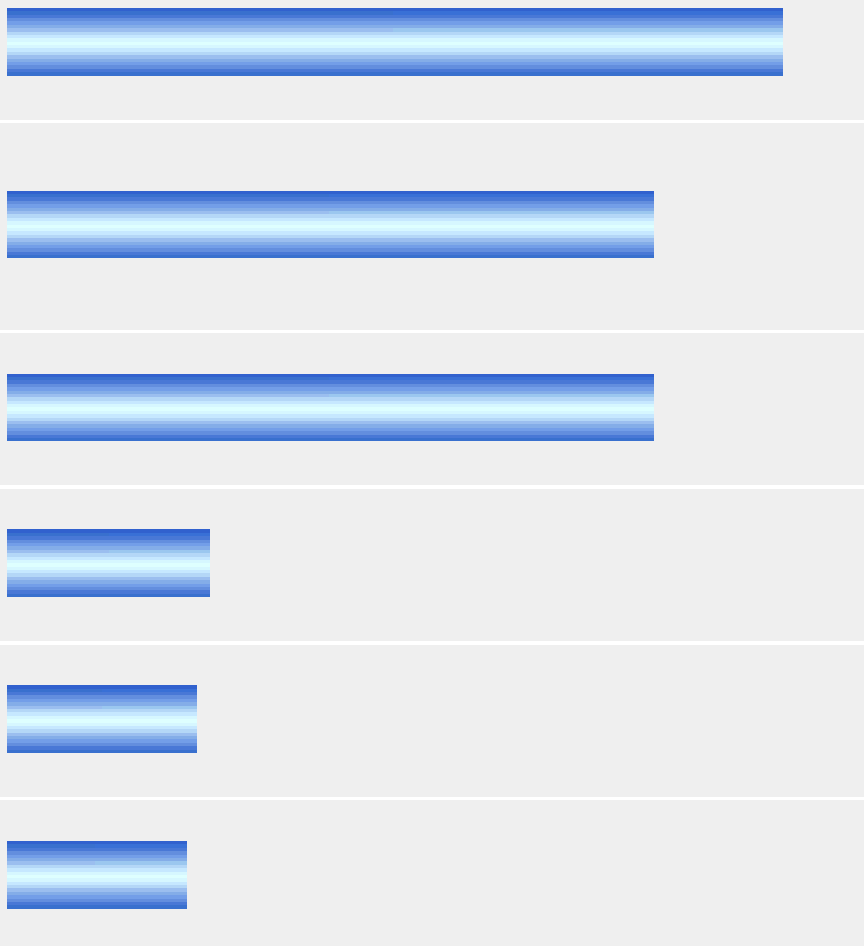
Gründe für die Ablehnung vorausbezahlter Systeme

- möchte nicht in Vorlage treten (57,1%)
- Risiko des Verlustes (44,2%)
- Intransparenz des Verfahrens (27,6%)
- zu aufwendig (25%)
- kein Zusatznutzen ersichtlich (24,6%)
- unbekanntes System (24,3%)

Was würden Sie tun, um mehr persönliche Sicherheit beim Bezahlen zu erlangen?

Angaben in %

Extra Software installieren	61,3
Längere Wartezeit beim Bezahlvorgang in Kauf nehmen	51,7
Bei einer Vertrauensstelle anmelden	51,4
Zusätzliche Hardware anschaffen	16,2
Mehr persönliche Daten angeben	15,8
Zusätzliche Kosten akzeptieren	14,9



Was macht Online-Shopping noch attraktiver?

Angaben in %

Mehrfachnennungen möglich

Eigenschaften eines guten Shops

Antworten: sehr wichtig

Fazit von IZV4

- Auch wenn der Verbraucher Verbesserungsbdarf bei Bezahlsystemen und Shops sieht, hindert ihn dies bisher nicht am Eínkauf
- insbesondere Verbraucherschutz ist ein Anliegen der Konsumenten, gute Bezahlsysteme sind nur ein Aspekt unter vielen (Rechtssicherheit, Umgang mit vertraulichen Daten etc.)
- selbst zwei Drittel der Skeptiker des Online-Shopping sehen sich in spätestens zwei Jahren regelmäßig im Internet einkaufen
- es wird nicht ein Bezahlverfahren der Zukunft geben. Maßgeblich ist für den Verbraucher auch eine breite Palette von Zahlsystemen, die je nach Situation gewählt werden kann
- neue Dienste und Produkte können den innovativen Bezahlsystemen den Weg ebnen

Kategorisierung nach Summe pro Transaktion

Picopayment

bis zehn Pfennig, Teilungen bis hundertstel Pfennig

Micropayment

bis fünf Mark, Teilungen bis ein Pfennig

Macropayment

Beträge ab fünf Mark, Teilungen bis ein Pfennig

Probleme einer Finanztransaktion über ein offenes Netz

Verlust der Vertraulichkeit

Informationsgewinn durch einen Lauschangriff

Verlust der Integrität

Stimmen die empfangenen Nachrichten mit den versendeten überein?

Verlust der Authentizität

Sind sich Sender und Empfänger einander sicher?

Verbindlichkeitsverlust

Ist der Vertrag verbindlich?

Unterschiedliche Anforderungen an ein Zahlungssystem

Kauf von Inhalten/Datenbanknutzung

einfache Bedienung, keine zusätzlichen Kosten, spontan nutzbar, anonym

Kauf von Büchern

Rückabwicklungsmöglichkeit, einfache Bedienung, keine zusätzlichen Kosten, spontan nutzbar

Wertpapierhandel

mehr Sicherheit der Transaktion, Schutz der persönlichen Daten, einfache Handhabung (steht nicht im Vordergrund), Schnelligkeit der Ausführung

Kauf von einem Liter Milch

schnell, einfach, ohne extra Kosten, spontan nutzbar

Unterschiedliche Anforderungen an ein Zahlungssystem

Kauf von Inhalten/Datenbanknutzung

hohes Maß an Vertraulichkeit, einfache Handhabung, schnelle Abwicklung

Kauf von Büchern

Stornierungsmöglichkeit, geringe Transaktionskosten

Wertpapierhandel

besonders große Sicherheit, hohes Maß an Vertraulichkeit

Kauf von einem Liter Milch

wenig Sicherheit, wenig Vertraulichkeit, schnelle Transaktion, geringe Transaktionskosten

Möglichkeiten einer Zugangsprüfung

Überprüfung personenbezogener Merkmale

Unterschrift, Fingerabdruck

Inhaberbezogene Kriterien auf Hardwarebasis

Chipkarte(nleser), bestimmte Hardware (z.B. Dongle)

Inhaberbezogenes Wissen

Geheimnummern, Passwörter

Lastschrift

- Anbieter: jede Bank
- einfach
- hoher Verbreitungsgrad
- Händler bestimmt Einziehungszeitpunkt
- Ohne Unterschrift (eigentlich) Verstoß gegen das Lastschriftabkommen, die erste Bestellung müßte per Fax/Post mit Unterschrift erfolgen.
- Kunde hat sechs Wochen Zeit, die Lastschrift zurückzufordern.
- Für den Händler ist bei Vertragsabschluss unklar, ob das Konto existiert oder eine Deckung besteht.
- nur in Deutschland einsetzbar
- Kosten pro Transaktion etwa 30Cent

Kreditkartenunternehmen in die Pflicht genommen

29.05.2002 – intern.de

Der Bundesgerichtshof hat bereits am 16. April eine Entscheidung getroffen, die den Betreibern von Online-Shops sehr entgegen kommt. Sie tragen zukünftig nicht mehr alleine das Missbrauchsrisiko, wenn bei einer Bestellung in betrügerischer Absicht eine Kreditkartennummer angegeben und der Kauf vom Inhaber der Karte storniert wurde.

http://www.haerting.de/deutsch/archiv/BGH-Kreditkarte.pdf

http://home.t-online.de/home/dietmar.beining/visa.htm

http://www.recht-in.de/urteile/urteil.php?urteilID=50167

Es ist ein offenes Geheimnis, dass Kreditkarten nirgendwo sonst so häufig missbraucht werden, wie im Internet. Wie vor Tagen berichtet, werden Kreditkarteninformationen mittlerweile in großem Stil gehandelt, um sie für Betrügereien im Internet zu verwenden.

http://www.intern.de/news/2896.html

Die Händler, die Zahlungen via Kreditkarte akzeptieren, haben dabei einen denkbar schlechten Stand. Sie müssen zunächst im Fall einer Online-Bestellung eine Service-Gebühr an die Kreditkartenunternehmen zahlen, die meist höher ist, als beim Ladenkauf. Sie stehen aber gleichzeitig voll für den Schaden ein, der bei einem Missbrauch entsteht.

Entdeckt ein Kreditkarteninhaber einen Missbrauch, kann er die Abbuchung rückgängig machen und das Kreditkartenunternehmen verlangt ebenfalls die bereits ausgezahlte Kaufsumme vom Händler zurück. Die Ware ist dann in vielen Fällen weg und der Händler trägt den Schaden selbst.

Die Kreditkartenunternehmen konnten sich dabei auf eine Entscheidung des VIII. Zivilsenats des BGH aus dem Jahr 1990 stützen (VIII ZR 139/89). Demnach handelt es sich bei dem Vertragsverhältnis zwischen Kreditkartenunternehmen und dem Vertragsunternehmen um einen Forderungskauf.

Von dieser Auffassung rückte der XI. Zivilsenat nun ab (XI ZR 375/00). Wie üblich in solchen Fällen, wurde an den ursprünglich urteilenden VIII. Zivilsenat zunächst die Anfrage gestellt, ob dieser an seiner Rechtsauffassung festhält. Dem war nicht so, denn sonst wäre es zu einer Vorlage an den Großen Senat gekommen. Nach Auffassung des XI. Zivilsenats handelt sich bei dem Vertragsverhältnis nicht um einen Forderungskauf, sondern um ein "abstraktes Schuldversprechen".

Die einseitige Belastung des Händlers hat der BGH im übrigen in seinem neuen Urteil für unangemessen und unwirksam erklärt. Zukünftig müssen die Kreditkartenunternehmen im Missbrauchsfall zumindest teilweise für den Schaden aufkommen.

Das Urteil dürfte weitreichende Konsequenzen haben. Die Kreditkartenunternehmen mussten bisher in Sachen Online-Sicherheit keine allzu großen Bedenken haben. Den entstehenden Schaden mussten sie ja nicht selbst tragen. Das dürfte sich nun zumindest in Deutschland dramatisch ändern. Die Kartenunternehmen sollten nun ein wesentlich größeres Interesse haben, Missbräuche im Internet zu verhindern.

Kreditkartenzahlungen

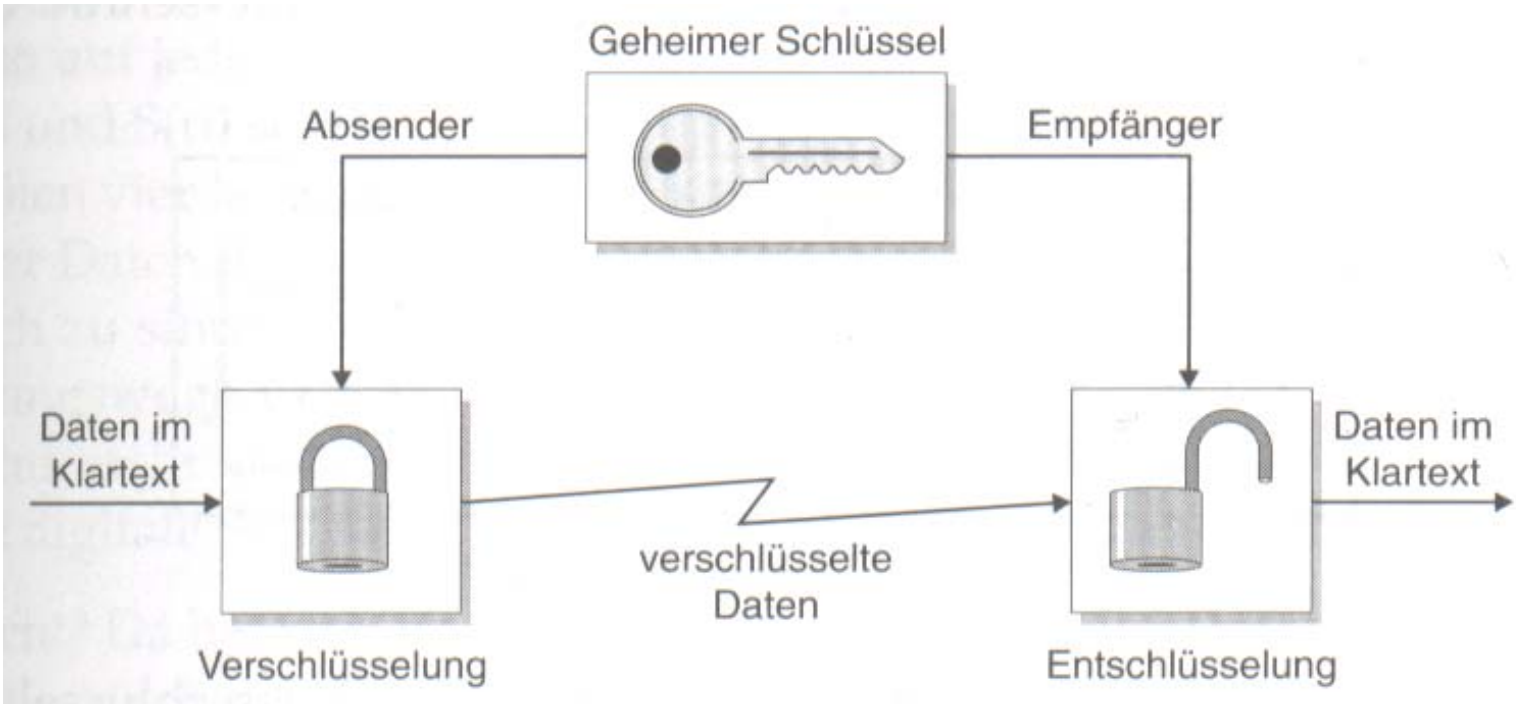
Unverschlüsselte Übertragung der Kreditkartendaten

Verschlüsselte Übertragung der Kreditkartendaten

Verifizierung/Authentitätsprüfung über Clearingstelle

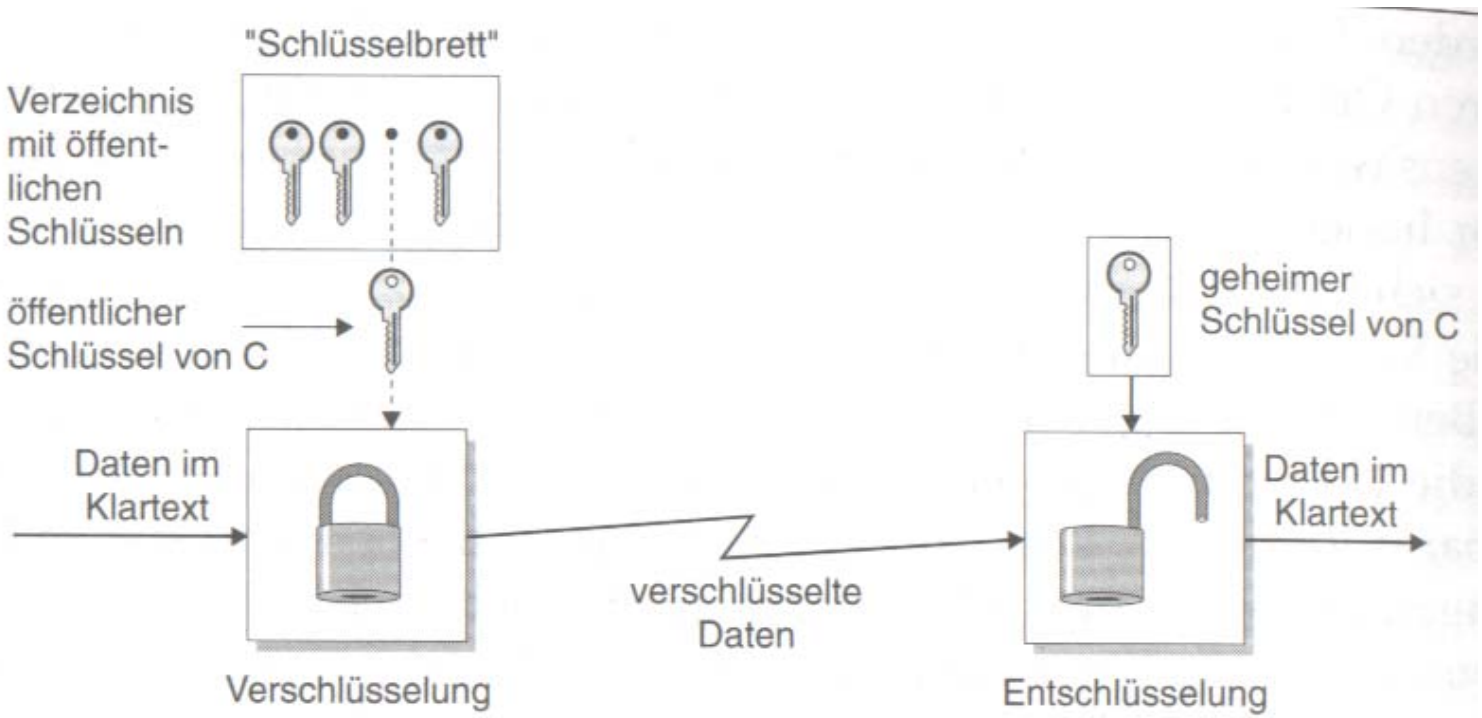
Verschlüsselungsverfahren

Symmetrisches Verschlüsselungsverfahren

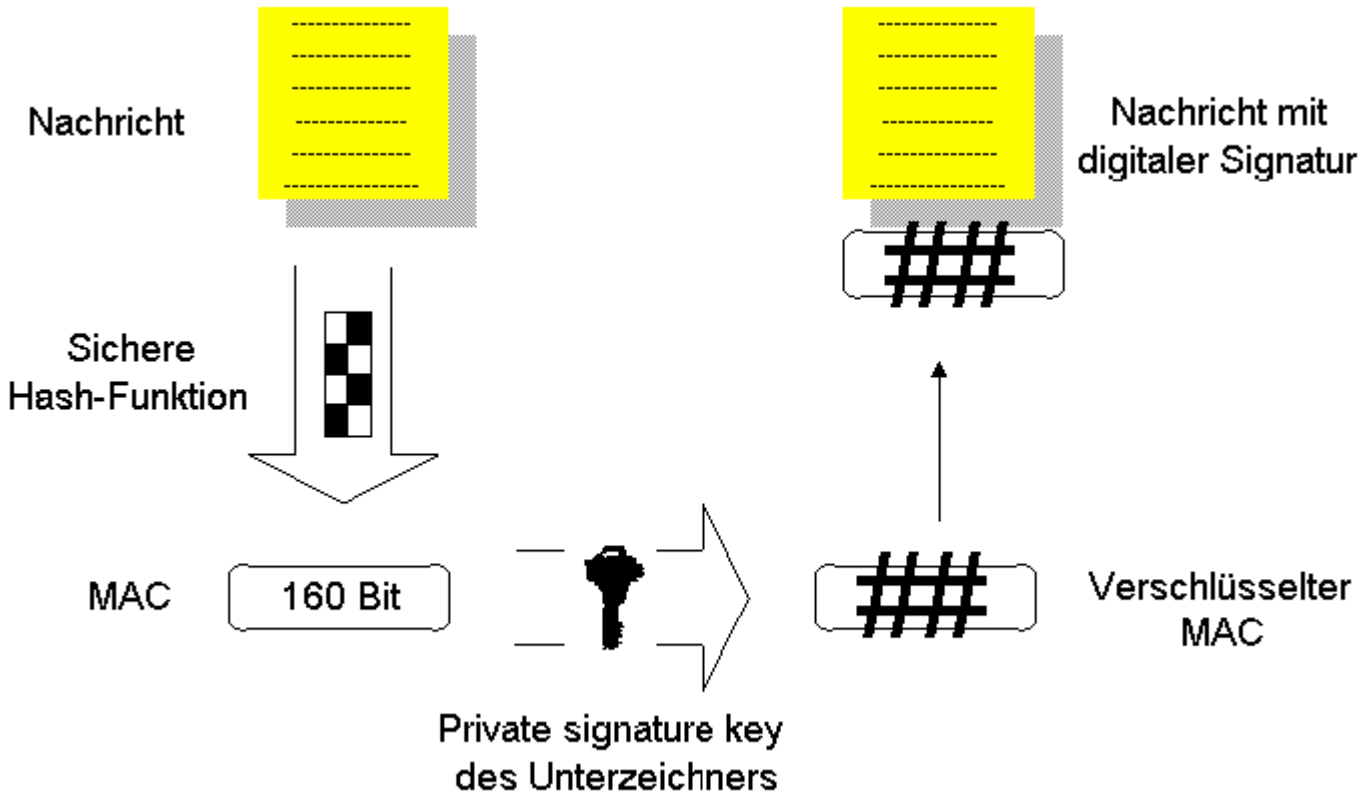


Nachteil: Schlüssel muss „geheim“ übertragen werden
Vorteil: schnell und sicher

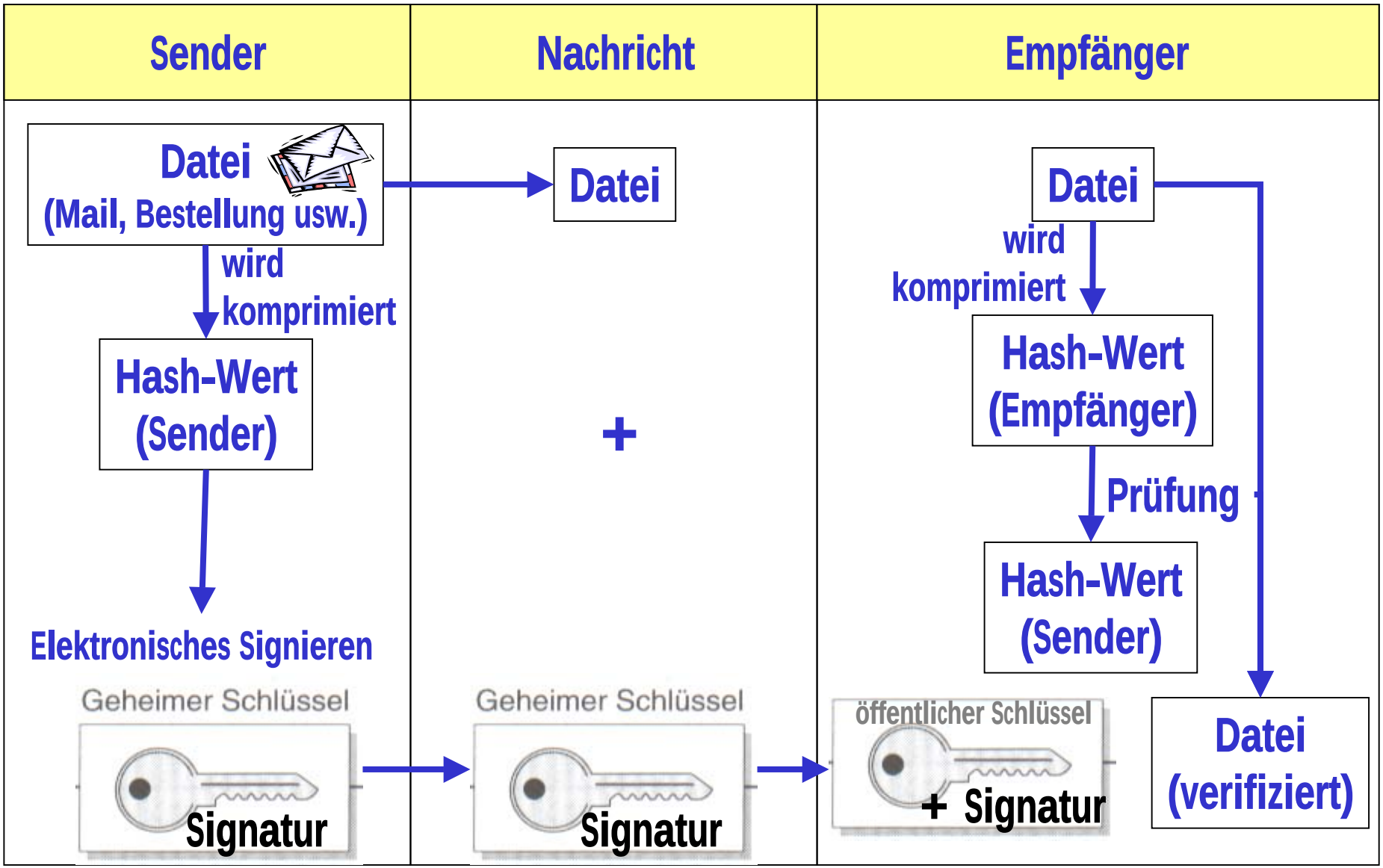
Asymmetrisches Verschlüsselungsverfahren
Public Key Verfahren



Digitale Unterschrift



Digitale Unterschrift



SSL - Secure Socket Layer

- ursprünglich von Netscape entwickelt
- besteht aus Record-Protokoll (Definition des Formates, in dem Daten übertragen werden) und Handshake-Protokoll (Authentifizierung der Kommunikationspartner)
- Handshake-Protokoll: Browser und Server „verständigen“ sich über das zu verwendende Verschlüsselungsverfahren
- https://

View A Certificate - Netscape

This Certificate belongs to:
www.my-world.de
Terms of use at www.verisign.com/RPA
(c)99
Multimedia DV-Hochtechnologie
Karstadt AG
Theodor-Althoff-Str. 2, D-45133 Essen,
Nordrhein-Westfalen, DE

This Certificate was issued by:
Secure Server
Certification Authority
RSA Data Security, Inc.
US

Serial Number: 2F:E6:34:F0:31:D3:51:31:8B:06:CF:04:5D:7B:43:DC
This Certificate is valid from Wed Nov 17, 1999 to Sat Nov 25, 2000
Certificate Fingerprint:
DA:EA:7F:F6:BA:47:2B:20:2D:73:D2:2B:17:F7:0C:4F

OK

Vorteile

- Absolut einfach bedienbar auf Kundenseite
- Auf Kundenseite lediglich Browser notwendig
- Keine Anmeldung erforderlich
- Über 1 Mrd. potentielle Nutzer weltweit (= Anzahl Kreditkarteninhaber)
- Einfach auf Händlerseite in bestehende Backoffice-Systeme integrierbar
- Auf Händlerseite Nutzung vorhandender Autorisierungs- und Clearingsstrukturen

Risiken

- Transaktion nicht nachweisbar (weder dem Kunden noch dem Händler)
- Transaktion beim Händler jederzeit manipulierbar (Betrag, Währung, Zahlungsmodalitäten)
- allein Wissen um Kreditkartennummer und Verfallsdatum ermöglicht Missbrauch

SET
Secure Electronic Transaction

aus **STT** (Secure Transaction Technology) von Visa und Microsoft

und **SEPP** (Secure Electronic Payment Protocol) von MasterCard, IBM, Netscape und Cybercash

entstand SET (Februar 1996)

Ziele von SET

1. Garantie der Vertraulichkeit von Informationen (durch Nachrichtenverschlüsselung)
2. Garantie der Integrität von Zahlungen (durch digitale Unterschrift)
3. Garantie der Identität des Karteninhabers (durch digitale Unterschrift mit Zertifikat)
4. Garantie der Identität des Händlers (durch digitale Unterschrift mit Zertifikat)
5. Verwendung bestmöglicher Sicherheitssysteme während eine Transaktion
6. Gewährleistung größtmöglicher Kompatibilität aller SET-Systeme auf allen Plattformen

Voraussetzungen für SET

für Kunden

- SET-Software („Wallet“) mit den Daten der genutzten Karten
- SET-Zertifikat (wird bei der Bank bentragt und enthält Zugangsdaten)

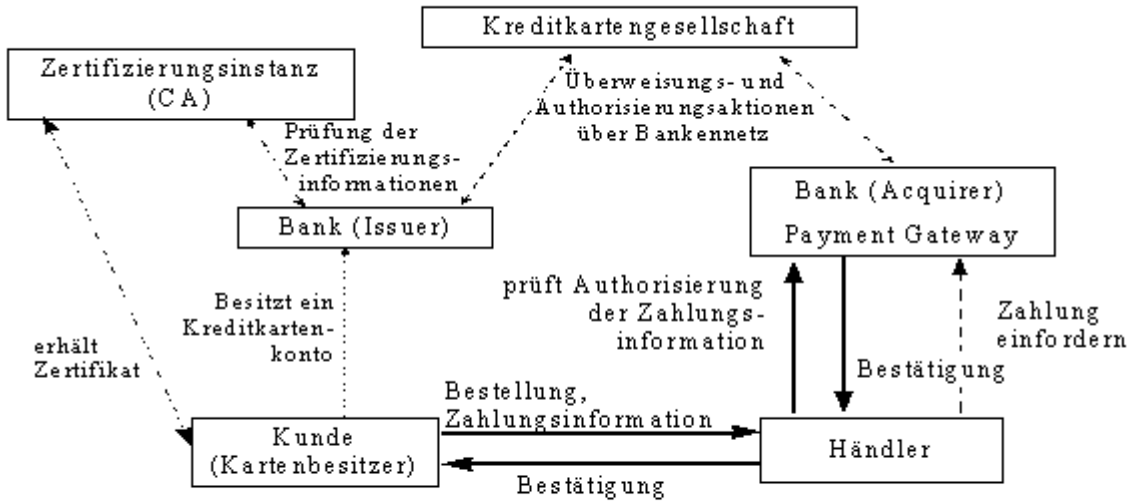
für Händler

- SET-Händlerzertifikat

für Banken

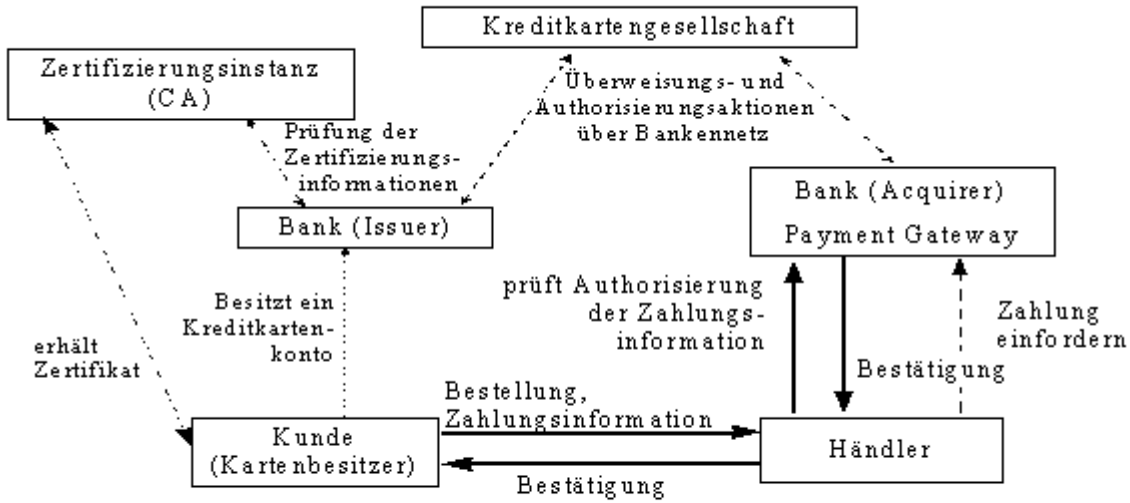
- SET-Payment-Gateway (Schnittstelle zwischen Internet und den Autorisierungsnetzen der Kartengesellschaften)
- SET-Zertifikat der Kreditkartengesellschaften

Zahlungsabwicklung nach dem SET-Protokoll



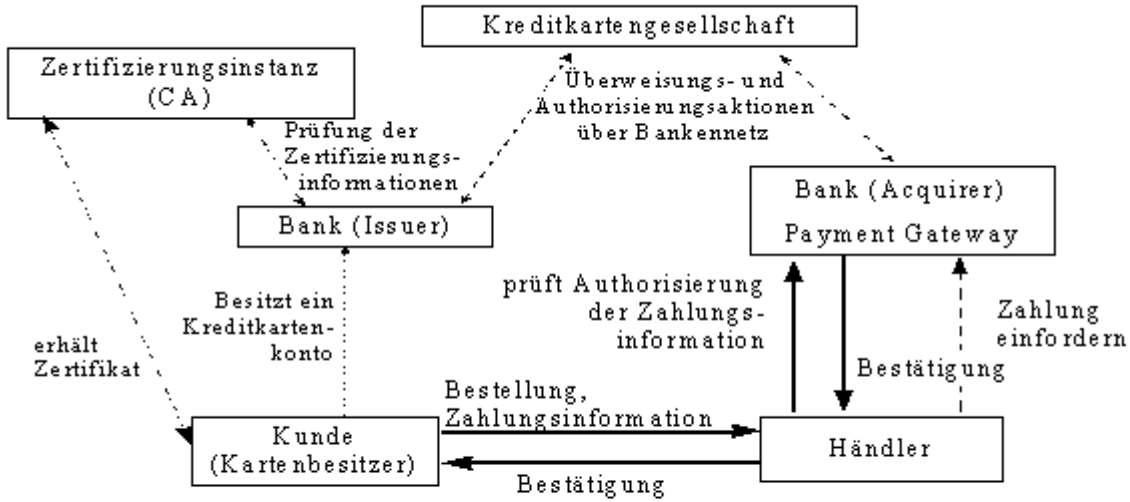
1. Initialisierungsnachricht Kunde an Händler
2. Händler sendet digital signierte Nachricht, die zusätzlich das Verschlüsselungszertifikat mit dem öffentlichen RSA-Schlüssel der Zertifizierungsstelle/Kreditkarteunternehmen/Clearing Stelle enthält.
3. Kunde fertigt signierte Bestellung und signierte Zahlungsanweisung an. Keditkartendaten werden mit dem öff. RSA-Schlüssel verschlüsselt, sind also durch den Händler nicht lesbar.

Zahlungsabwicklung nach dem SET-Protokoll



4. Händler schickt eine digital signierte Anfrage (erst DES [symmetrisches Verfahren] verschlüsselt und dann RSA verschlüsselt), dazu kommt das Verschlüsselungszertifikat des Händlers, die Zahlungsanweisung und der verschlüsselte DES-Schlüssel.
5. Die Kreditkartenfirma entschlüsselt die Nachricht und authorisiert die Zahlung.
6. Der Händler erhält eine Bestätigungsnachricht.

Zahlungsabwicklung nach dem SET-Protokoll



Drei Phasen der SET-Transaktion

1. Bestellung (*Purchase Request*)
Bestellung des Kunden und Quittung des Händlers
2. Authorisierung (*Payment Authorisation*)
Anfrage des Händlers an seine sog. Zertifizierungsstelle (*Payment Gateway*), ob die Zahlungsanweisung des Kunden akzeptiert wird
3. Abrechnung (*Payment Capture*)
Abrechnung des Händlers mit der Bank des Kunden

Akzeptanzprobleme

- **Bisher kaum Nachfrage in den USA**
- **Aufwand für Karteninhaber immer noch hoch**
- **Aufwand und Kosten für Händler bisher zu hoch**
- **alternative Softwareangebote verunsichern Händler**
- **bisher kaum Marketingmaßnahmen**
- **in Deutschland z.Zt. etwa 15 Tsd. Nutzer und 100 Händler**

Kosten (Beispiel mit HypoVereinsbank)

Freischaltung	DM 1.500,00 einmalig
Hosting-Service	DM 150,00 p.m.
Transaktion	1% vom Umsatz
(SET-Zertifikat	bis DM 500,00 p.a.) im Hosting enthalten
Servicegebühr	3,90%

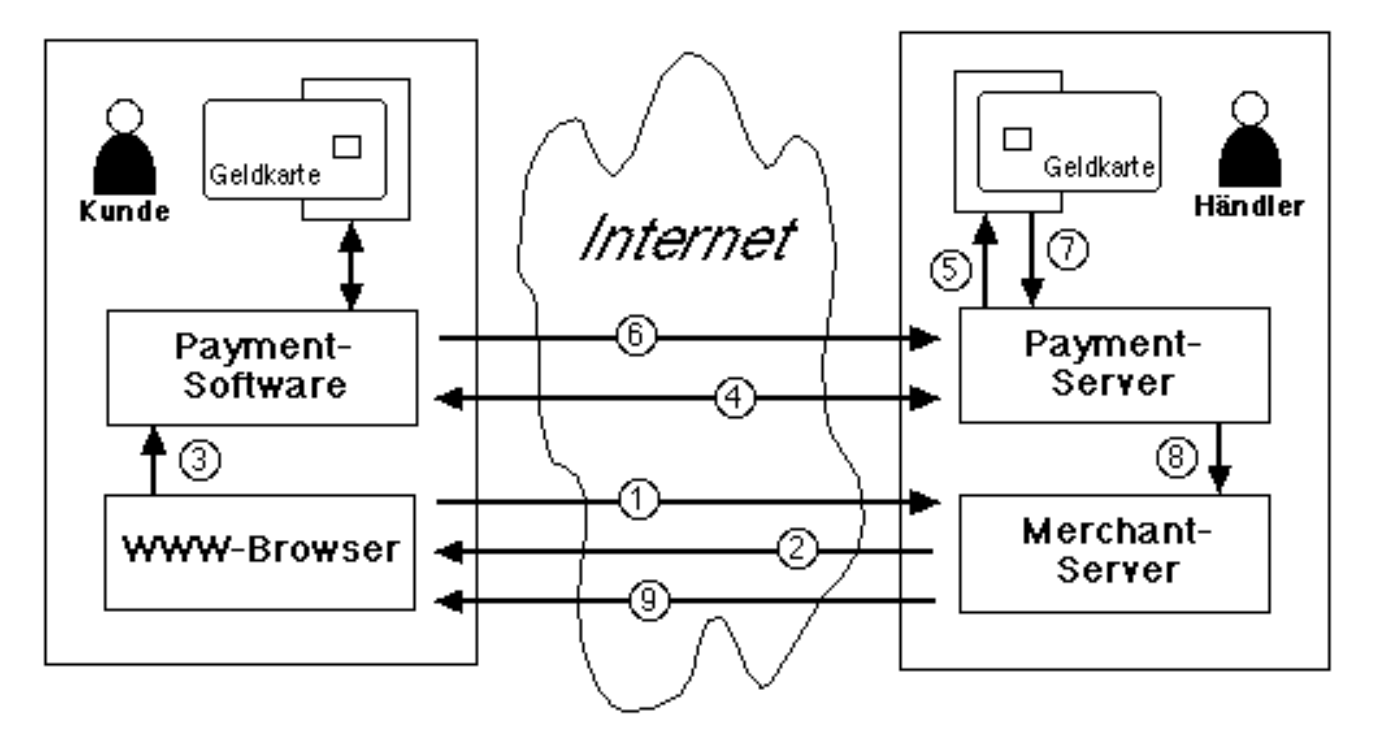
SET/SSL

- **Kunde übermittelt per SSL seine Kreditkartendaten an den Händler, Händler reicht die Daten per SET an die Kreditkartenfirma weiter**
- **Online-Überprüfung der Daten**
- **hohe Verbreitung gerade bei größeren Unternehmen/höheren Kaufsummen**

Bezahlen per Geldkarte im Internet
Beispiel Sparkasse

- Voraussetzung: Kartenlesegerät (seriell oder USB), Geldkarte, Software
- 40 bis 50 Mio. Geldkarten im Umlauf, nur 0,1% der Inhaber nutzen sie

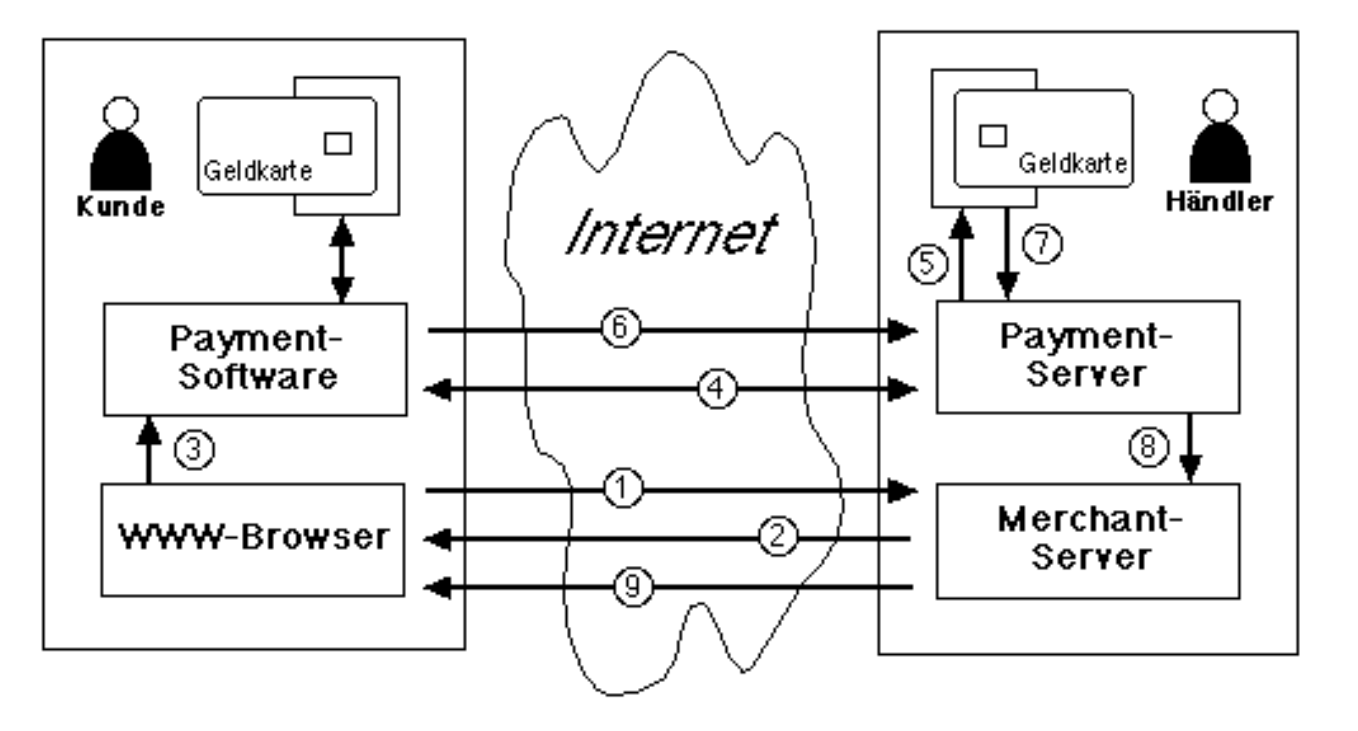
Die GeldKarte im Internet



Grafik: Institut für Wirtschaftspolitik unf Wirtschaftsforschung, Uni Karlsruhe

1. Kunde bestellt Ware
2. Händler übersendet elektronische Rechnung
3. Kunde bestätigt den Betrag mit seiner Software
4. Die Zahlung wird über die Software von Händler und Kunden eingeleitet
5. Der Payment-Server des Händlers übermittelt Details der Zahlungen an die Händler-Karte

Die GeldKarte im Internet



Grafik: Institut für Wirtschaftspolitik unf Wirtschaftsforschung, Uni Karlsruhe

6. Karten authentifizieren sich gegenseitig, Zahlung wird vollzogen, Geldkarten protokollieren Transfer

7. Karte des Händlers meldet erfolgreiche Zahlungen an den Payment-Server

8. Payment-Server reicht Quittung der Zahlung an den Merchant-Server weiter.

9. Die Auslieferung der Ware wird vom Payment-Server autorisiert.

Net900

- Micropaymentsystem
- Abrechnung über die Telefonrechnung oder per Bankeinzug (KONTOPASS) – Entscheidung bei Installation der Software
- „Nachfolger“ des Inkassosystems von T-Online
- spezielle Software notwendig (400 kB)
- aktuelle Datenverbindung wird unterbrochen und kostenpflichtige Verbindung wird aufgebaut
- anschließend wird ursprüngliche Datenverbindung wieder aufgebaut
- Zahlung „pay per click“ oder „pay per minute“
- Summen bis 4,99 DM pro Zeiteinheit/Transaktion möglich
- Geheimnummer für Kontopass wird per „Überweisung“ mitgeteilt

Bezahlen über Handy paybox

Grafik: Paybox

1 Der Kunde füllt den Warenkorb im Internet, wählt „Paybox - Zahlen per Handy" und gibt seine Mobiltelefonnummer oder einen Alias an

2 Paybox verbindet die Transaktions-partner und stellt die Verbindung zum Han-dy des Kunden her

3 Der Kunde autorisiert den Betrag und die Zahlung an den Internet-Shop...

4 ...durch Eingabe der Paybox-PIN auf seinem Handy

5 Der Ausgleich der Rechnung erfolgt per Lastschrift-einzugs-verfahren

Bezahlen über Handy
paybox

Vorteile

Wenig Missbrauchsmöglichkeiten (nur von angeschaltetem Mobiltelefon mit angegeber SIM-Karte/Nummer kann bezahlt werden)
Missbraucher bräuchte Handy, Handy-PIN und paybox-PIN
Sperrung des paybox-Kontos bei Handyverlust
Echtzeit-Autorisierung
online und offline nutzbar
Peer-to-peer-Transaktion möglich
ca. 260 Tsd. Registrierte Nutzer und etwa 5000 Shops (on- und offline)

Nachteile

Nutzung nur für Handy-Besitzer möglich
mögl. Abhören der paybox-PIN möglich
Grundgebühr für Käufer, keine spontane Nutzung
Transaktionskosten für Händler 3-5%

Bezahlen über Handy
paybox

	Basic	Standard	Premium
Softwarelizenz	€ 500	€ 500	€ 2500
Jahresgebühr	€ 100	€ 100	€ 300
Servicegebühr	5%	3,5%	3%
Stornogebühr	€ 0,25	€ 0,25	€ 0,25
Gutschriftgebühr	€ 3	€ 3	€ 3
Vertragslaufzeit	6 Monate	12 Monate	6 Monate

Grafik: Franz Ecker & Partner, Bad Griesbach

Click & buy Firstgate

- Micropaymentsystem
- Kunde muss sich bei firstgate mit Konto- oder Kreditkartennummer registrieren (kostenlos)
- Kunde klickt kostenpflichtigen Link an, wird zum firstgate-Server geleitet, muss sich per Paßwort identifizieren und bekommt kostenpflichtige Inhalte angezeigt
- Abrechnung pro Besuch der Site und für Nutzungsdauer möglich
- monatliche Abrechnung von firstgate mit dem Kunden und dem Anbieter
- Provision zwischen 30% und 50%
- monatliche Gebühr für Anbieter: 9,90 DM
- ca. 260 Tsd. registrierte Nutzer, ca. 1700 Händler

iclear EuroCoin

- Idee: Minimierung des Ausfallrisikos bei Rechnungskauf
- Kunde muss sich bei iclear mit Kontonummer registrieren
- Kunde bezahlt im angeschlossenen Shop per Rechnung, Rechnung kommt von iclear und wird nach 14 Tagen vom Konto abgebucht
- Kosten: 3,5% Provision, 100€ Lizenzgebühren (andere Tarifmodelle möglich)
- überwiegend in kleineren Shops verbreitet
- nach eigenen Angaben 120 Tsd. Private Kunden und 1050 Shos

Zertifizierungsprogramme für Händler

- Ziel: Vertrauen schaffen
- Pflichten der teilnehmenden Unternehmen (Auswahl),
  größtenteils gesetzliche Bestimmungen:
  klare Nennung der Adresse
  gut sichtbarer Verweis auf AGBs
  verbindliche Preisangaben
  Einhaltung der Datenschutzbestimmungen
  verbindliche Lieferaussagen
  Auftragsbestätigungen
  Widerrufs- und Rückgaberecht
  Geld-Zurück-Garantie (trustedshops)
- bekannte Anbieter: trustedshops (Gerling-Konzern), shopinfo.net (EHI-Eurohandelsinstitut)

Anforderungen an elektronische Zahlungssysteme

Sicherheit

- Vertraulichkeit
- Transaktions-integrität
- Authentizität

Systemtechnik

- Verfügbarkeit
- einfache Benutzung
- Haltbarkeit
- Skalierbarkeit

Zahlungssystem (im engeren Sinn)

- Anonymität
- Akzeptanzfähigkeit
- Universalität
- Kompatibilität
- Internationalität
- Risikoverteilung
- Spontanität

Wirtschaftlichkeit

- Transaktionskosten
- Einstandskosten

Recht

- Verbindlichkeit
- bankrechtliche Anf.

Anforderungen an ein Zahlungssystem aus Kundensicht

- simple Benutzeroberfläche
- einfache Transaktionsabwicklung
- softwarebasiert
- problemlose Initialisierung der Software
- breite Akzeptanz
- Nutzung aller Kanäle
- der empfundene Sicherheitslevel muss hoch sein (nicht das objektive sondern das wahrgenommene Sicherheitslevel ist relevant)

Anforderungen an ein Zahlungssystem aus Händlersicht

- große Konsumentenbasis
- garantierte Zahlung
- minimale Eingriffe in bestehende Systeme
- Zuverlässigkeit

Anforderungen an ein Zahlungssystem aus Bankensicht

- Stärkung der Kundenbindung
- Profitabilität

Kriterien für die Auswahl eines Zahlungssystems

- Was für Produkte werden vertrieben?
- Wie hoch sind die Umsätze? pro Produkt/pro Kauf/insgesamt
- Umsatzvolumen pro Monat?
- Was für Kunden kommen überwiegend? Spontankäufer oder Stammkunden?
- nationale oder internationale Kunden?
- Ist eine Zahlungsgarantie notwendig?
- Wie wichtig ist die Beweisbarkeit/Dokumentation des Vertragsschlusses?
- Wie wichtig ist die Authentifizierung des Kunden?
- Wie hoch ist die Akzeptanz des Verfahrens?
- Wie hoch ist die Verbreitung?
- Welche Kosten verursacht das Verfahren? (fix und pro Transaktion)
- Welche Integrationsmöglichkeiten bestehen in den Shop?
- Welche Sicherheitsmechanismen werden benötigt?
- Werden die ausgewählten Verfahren von einem Unternehmen angeboten? Gibt es Zusatzleistungen?

Sicherheit

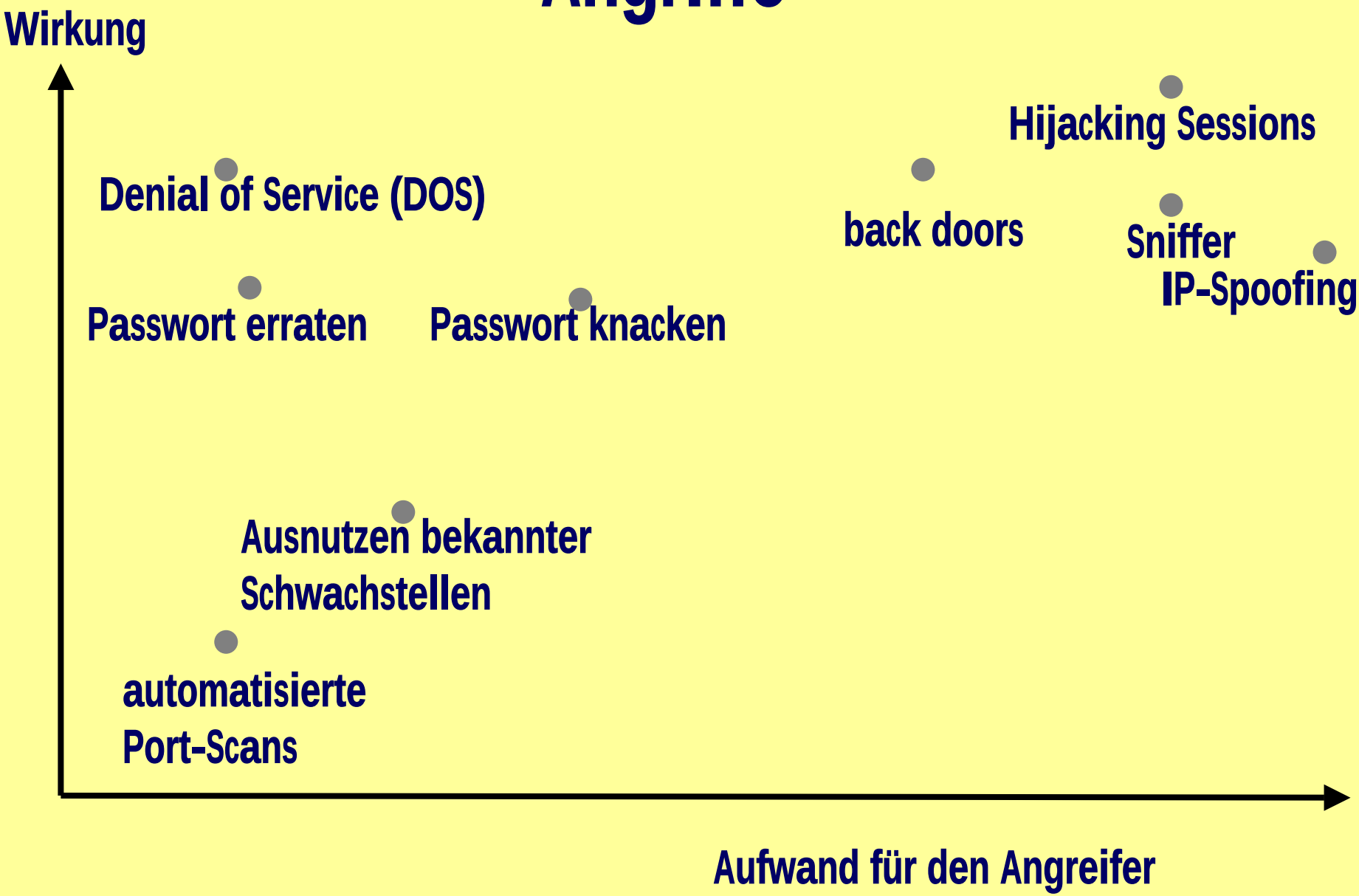
„Die technischen Voraussetzungen für die Fahrt mit Sicherheitsgurt auf der Datenautobahn liegen vor, es gilt ihn anzulegen.“

Ansgar Heuser, BSI

Entwicklung

- das Wissen der Angreifer hat kontinuierlich abgenommen, weil es Programme gibt, die Angriffsszenarien automatisch erzeugen
- Steigerung der Zahl der Angriffe
- überwiegende Zahl der Angriffe eher lästig als bedrohlich, da viele standardisiert sind und so mit einfachen Mitteln abgewehrt werden können
- drei Gruppen von Hackern
  - Ausleben des Spieltriebs/Ausprobieren von Tools
  - Demonstration ihrer eigenen Fähigkeiten und Sicherheitslücken der anderen
  - gezielt (von der Konkurrenz) beauftragte Spezialisten
- auf Grund der immensen Masse an Daten ist der Weg der Daten durch das Internet recht sicher (Paketprinzip), angreifbar sind Sender und Empfänger
- größte Gefahr immer noch: eigene Mitarbeiter, klassischer Diebstahl z.B. von Laptops

Angriffe


Wirkung
Hijacking Sessions
Denial of Service (DOS)
back doors
Sniffer
IP-Spoofing
Passwort erraten
Passwort knacken
Ausnutzen bekannter
Schwachstellen
automatisierte
Port-Scans
Aufwand für den Angreifer

Filtering Firewalls

- Filtern der eins- und ausgehenden Datenpakete
- Filtern nach IP-Adressen: bestimmte Nutzer können nichts raussenden und bestimmte Adressen können nicht angewählt werden
- Filtern nach Diensten/Protokollen: bestimmte Dienste können nicht genutzt werden, z.B. ftp, POP3-Mailing, IRC
- Filtern nach Virensignaturen
- Filtern nach Passwort

Proxy Server

- Vermittler zwischen internem und externem System
- verschleiert die internen IP-Adressen
- alle Datenpakete werden registriert und untersucht
- Speicherung häufig aufgerufener Web-Seiten
- Auswertung über Nutzerverhalten