Wie werde ich mein Geld los?

Wie kommt der Händler an sein Geld?

In der realen Welt

bar bezahlt werden
70% der Käufe

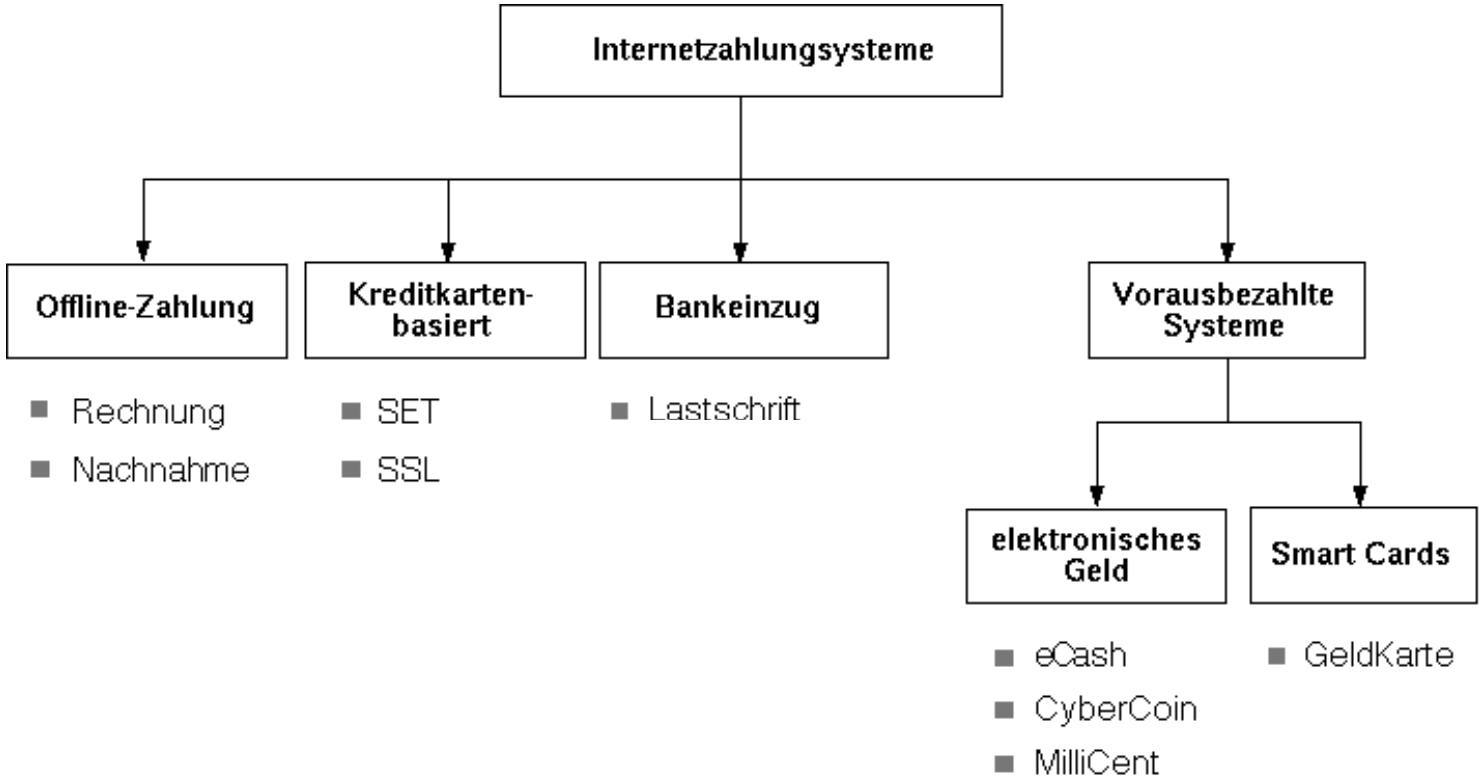
6% mit Schecks
19% kartengestützte Systeme

Eurocard: 70% aller Internet-Transaktionen werden über Kreditkarten abgewickelt. In Deutschland verfügen 17% über mind. eine Kreditkarte (Mobiltelefone 40%).

Kategorisierung der Bezahlsysteme

Pre-Paid-Systeme	Pay-Now-Systeme	Pay-Later-Systeme
Hardwarebasiert z.B. Geldkarte Softwarebasiert z.B. CyberCoins, eCash	Nachnahme (offline) Paybox	Kreditkartenbasiert Ungesichert SSL SET (Varianten) Inkaso/Billing Net900 Firstgate Click&buy Rechnung Überweisung Lastschrift

Kategorisierung der Bezahlsysteme



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
- 6759 Teilnehmer
- November 2000 bis zum Januar 2001
- nicht repräsentativ

TeilNehmer-Profil

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

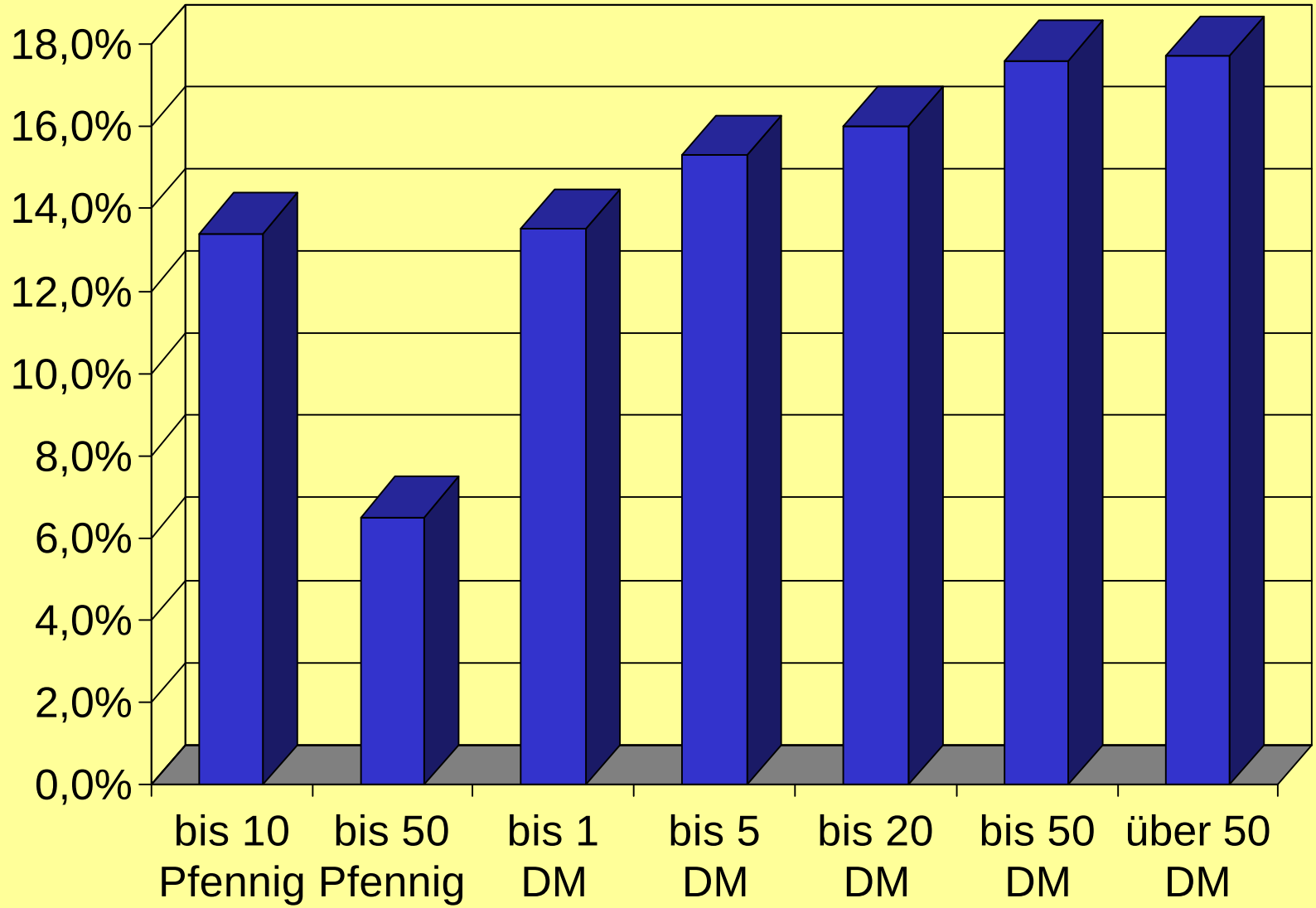
Fragen

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

Innovative BezahlIverfahren

- Pro Inkassosysteme 43,8%
- Pro vorausbezahlte Systeme 52,6%

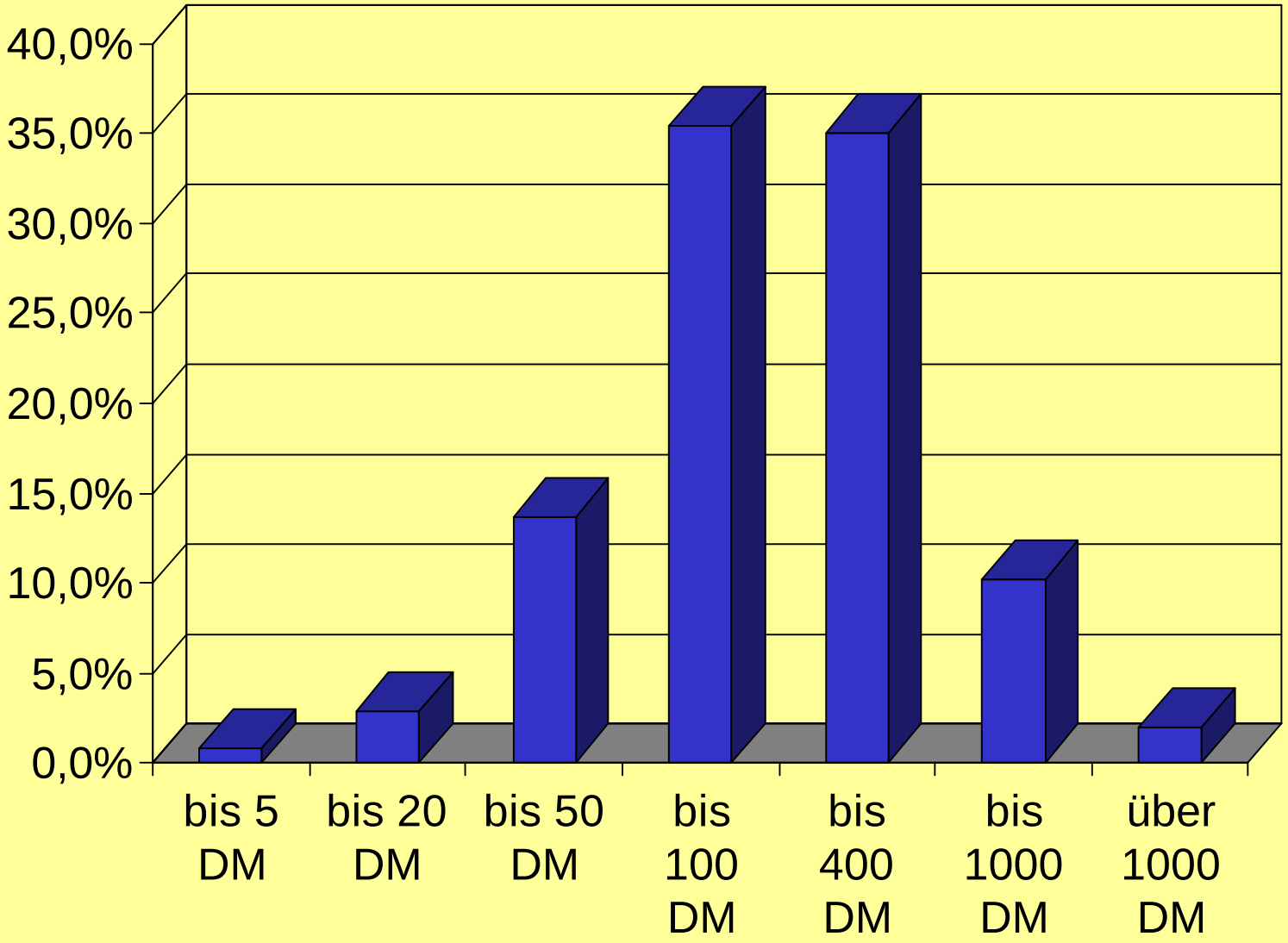
Maximaler Betrag pro Click bei Bezahlen mit Pay per Click



Bevorzugte Inkassounternehmen

- Banken (77,8%)
- Kreditkartenunternehmen (59,2%)
- Telekommunikationsunternehmen (46,1%)
- ISP (26,6%)
- unabhängige dritte Anbieter (19,2%)

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%)

Erfolgsfaktoren eines Zahlungssystems aus Verbrauchersicht

- möglichst keine Zusatzkosten durch Nutzung (70,6%)
- einfache Handhabung und Stornomöglichkeit (je 61,9%)
- Absicherung im Schadensfall und Belastungszeitpunkt – erst Ware dann Geld (59,1%)

Erfolgsfaktoren eines Online-Shops aus Verbrauchersicht

- vertraulicher Umgang mit Kundendaten (79,6%)
- keine unnötigen persönlichen Daten erheben (70,5%)
- bevorzugte Bezahlmethode muss angeboten werden (69,5%)
- verschlüsselte Internetverbindung (66,3%)
- klar verständliche AGBs (64,4%)

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

- digitale Signaturen einsetzen (75,6%)
- extra Software installieren (61,5%)
- längere Wartezeiten beim Bezahlen in Kauf nehmen (51,5%)
- bei einer Vertrauensstelle anmelden (51,5%)
- zusätzliche Hardware anschaffen (16,4%)
- zusätzliche Kosten akzeptieren (14,7%)

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 ebnenp

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?

Möglichkeiten einer Zugangsprüfung

Überprüfung personenbezogener Merkmale

Unterschrift, Fingerabdruck

Inhaberbezogene Kriterien auf Hardwarebasis

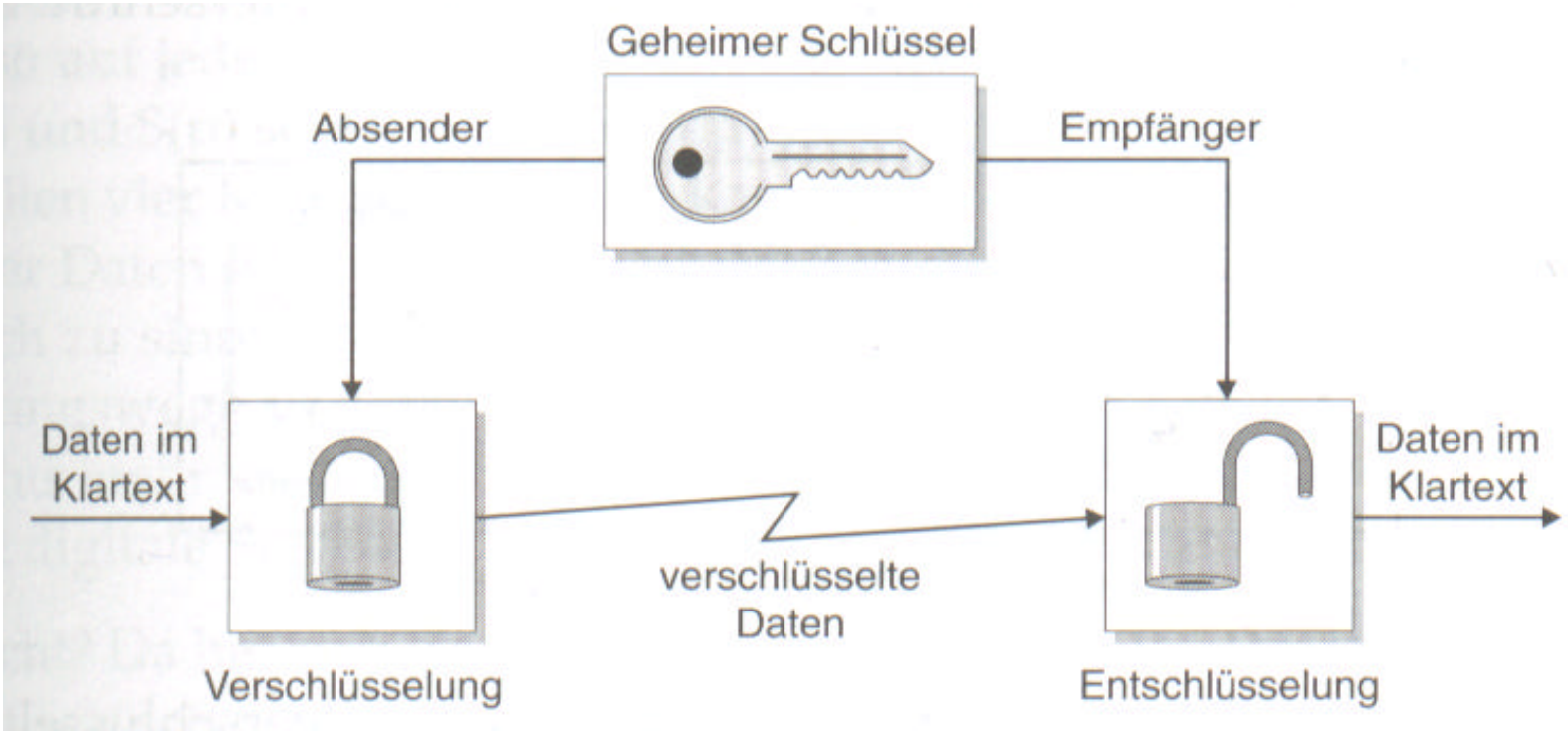
Chipkarte(nleser), bestimmte Hardware (z.B. Dongle)

Inhaberbezogenes Wissen

Geheimnummern, Passwörter

Verschlüsselungsverfahren

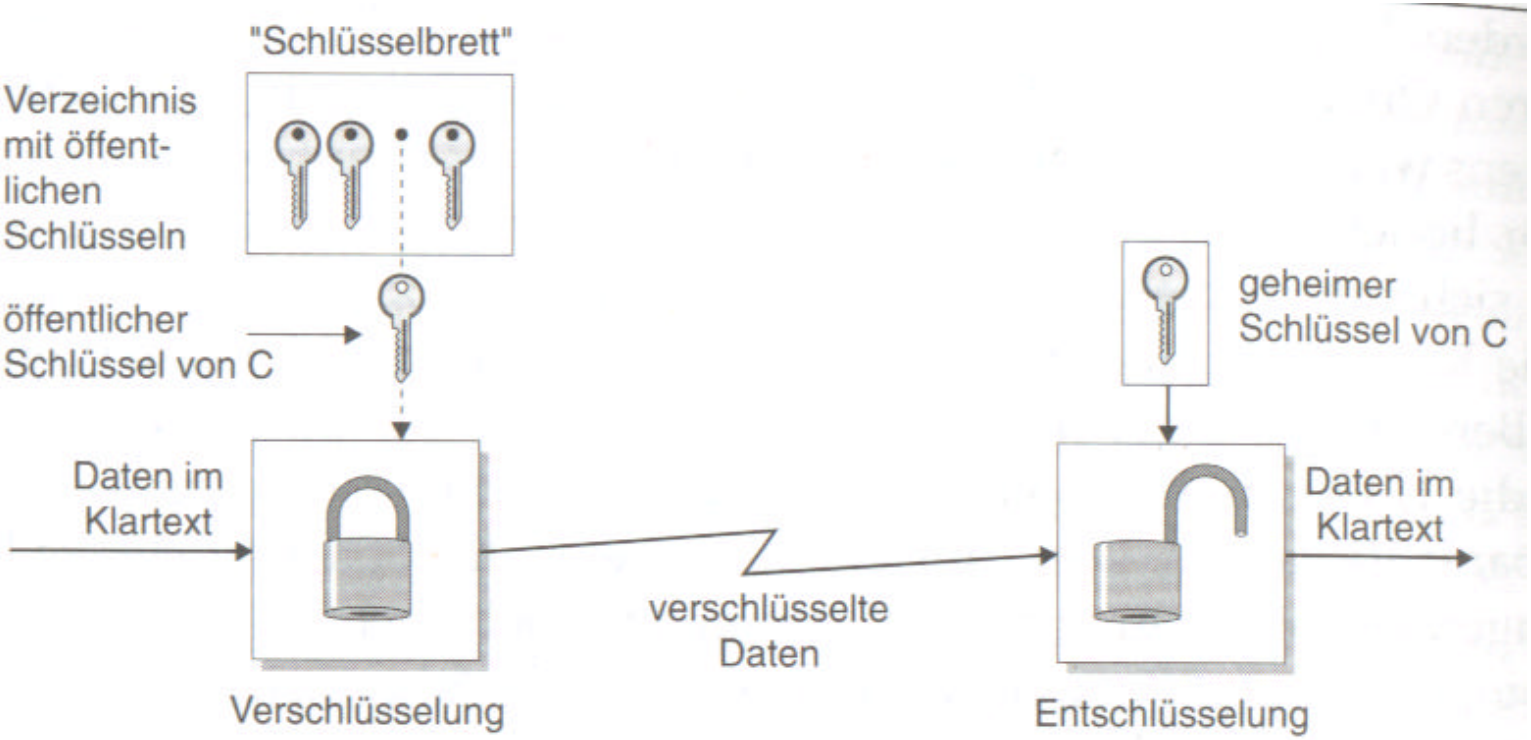
Symmetrisches Verschlüsselungsverfahren



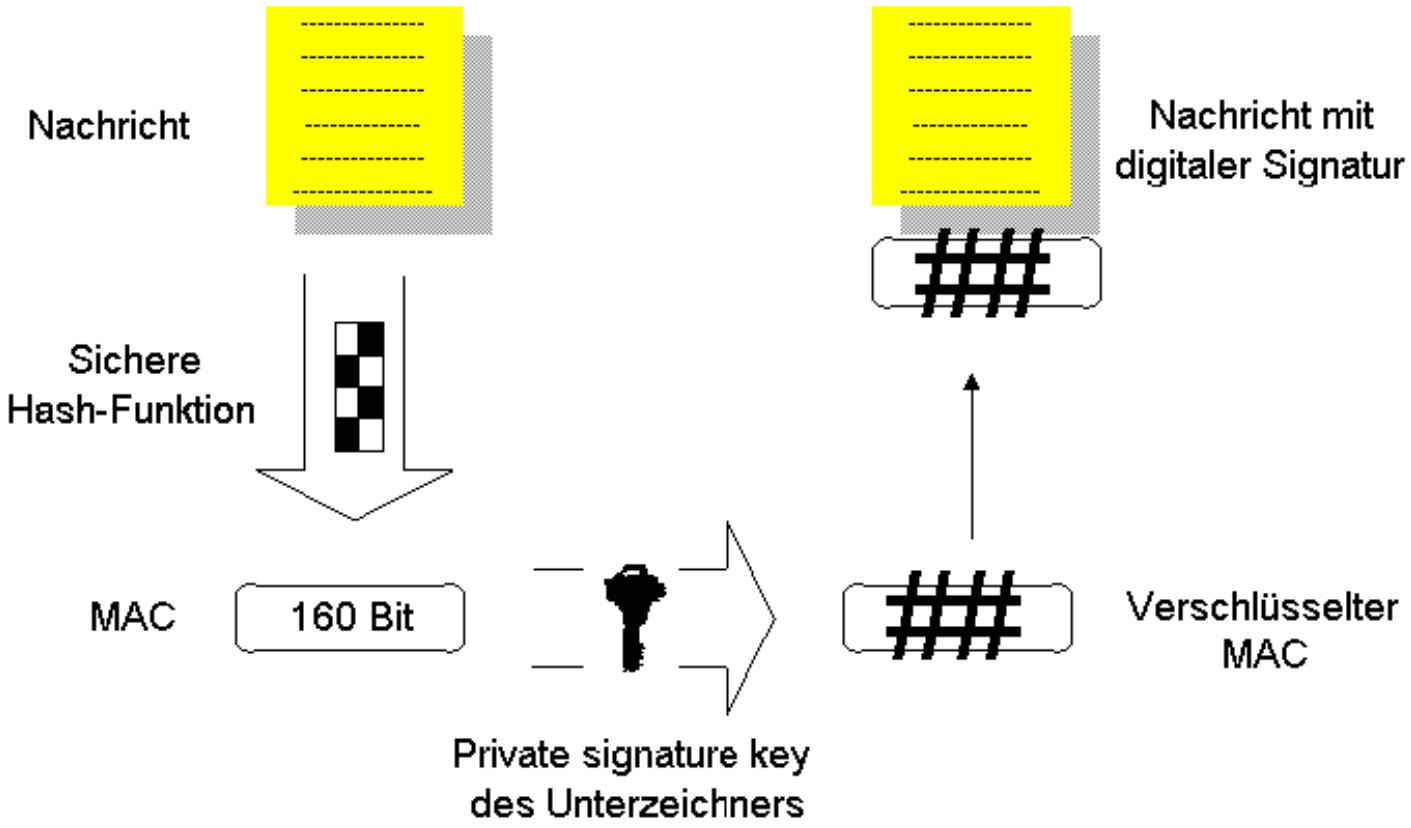
Nachteil: Schlüssel muss „geheim“ übertragen werden

Vorteil: schnell und sicher

Asymmetrisches Verschlüsselungsverfahren
Public Key Verfahren

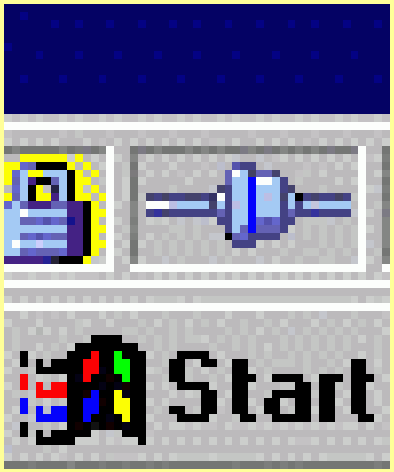


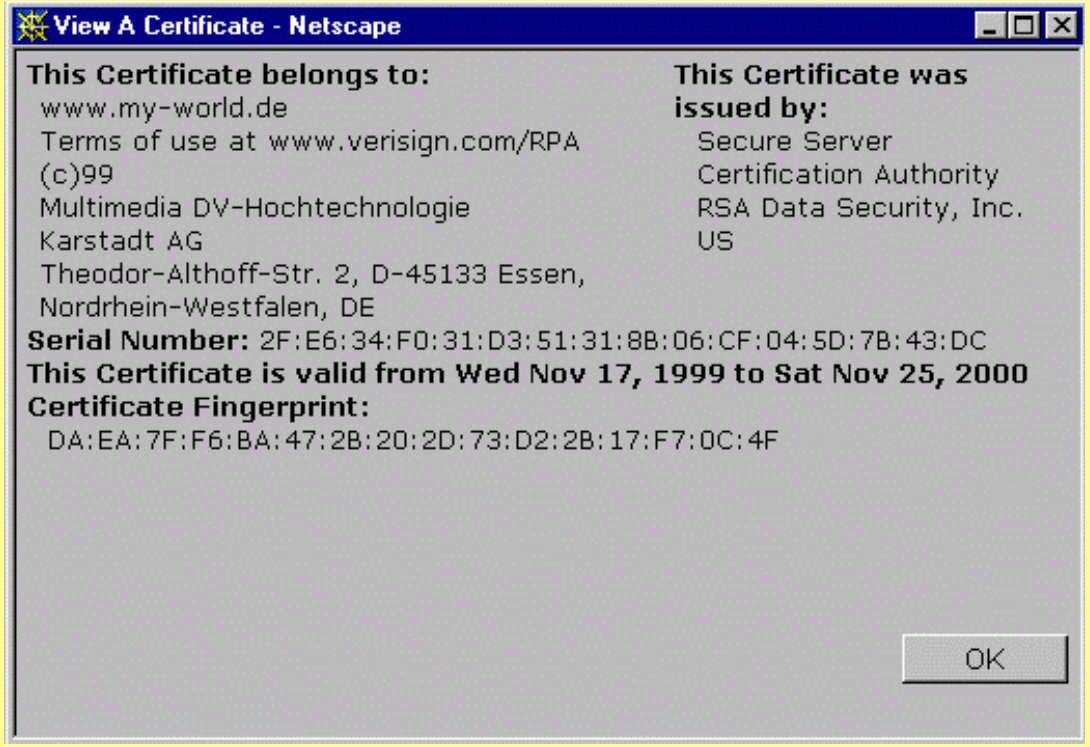
Digitale Unterschrift



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://





Vor- und Nachteile?

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

Beteiligte

- Kartenbesitzer (Cardholder)

  Jede Person, die eine Kreditkarte besitzt, und an SET teilnehmen möchte (oder schon teilnimmt)

- Kartenausgebende Bank (Issuer)

  Das ist das Unternehmen, das den Kartenbesitzer mit der Kreditkarte versorgt. Der Kartenaussteller ist letztendlich für die Begleichung der Schulden des Kartenbesitzers verantwortlich und trägt das Risiko

Beteiligte

- Händler (Merchant)

  Jede Institution, die Waren oder Dienstleistungen (Service) im Internet anbietet und sie an Kartenbesitzer verkaufen möchte

- Bank des Händlers (Acquirer)

  Der Acquirer besorgt die Kartenautorisierung und die Erfassung und Transferierung der Bezahlung für die Händler. Über Acquirer Akzeptanz mehrere Kreditkartengesellschaften möglich. Der Acquirer vergibt an Händler SET-Zertifikate

Beteiligte

- Payment Gateway

  Das Payment Gateway stellt eine Schnittstelle zwischen SET und den existierenden Netzwerken der Kreditkartengesellschaften dar, die zur Autorisierung und zur Erfassung der Wertausgleiche dient.

- Kreditkartengesellschaft (Brand)

  Stellen Regeln auf für Gebrauch und Akzeptanz von Kreditkarten. Sie unterhalten ein Netzwerk zur Autorisation der Bezahlungen und der Transferierung der Gelder

Beteiligte

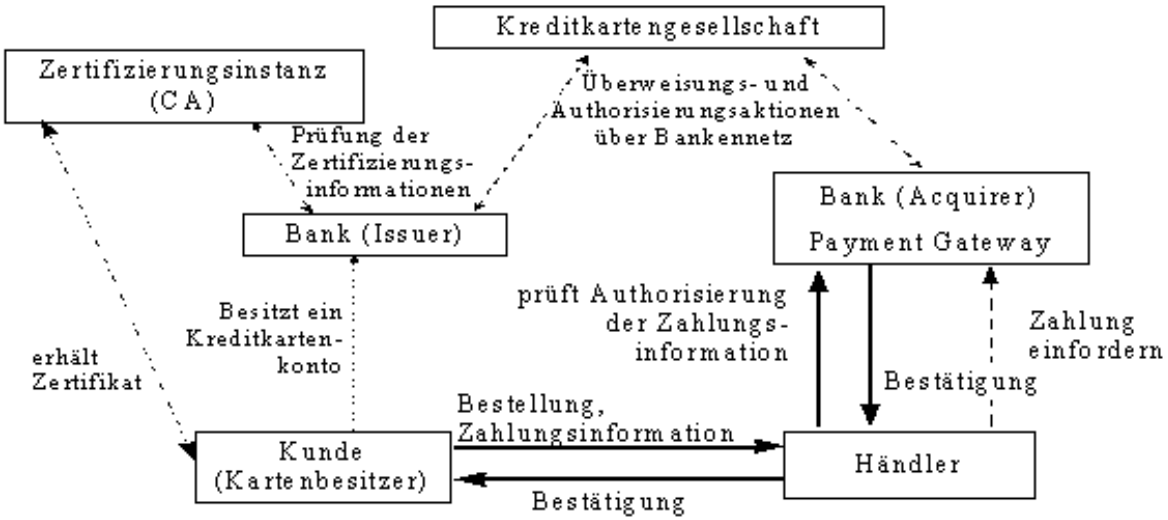
- Drittanbieter (Third Parties)

  Issuer und Acquirer können sich der Dienst von Drittanbietern zur Geschäftsabwicklung bedienen

- Zertifizierungsinstanzen (Certification Authorities)

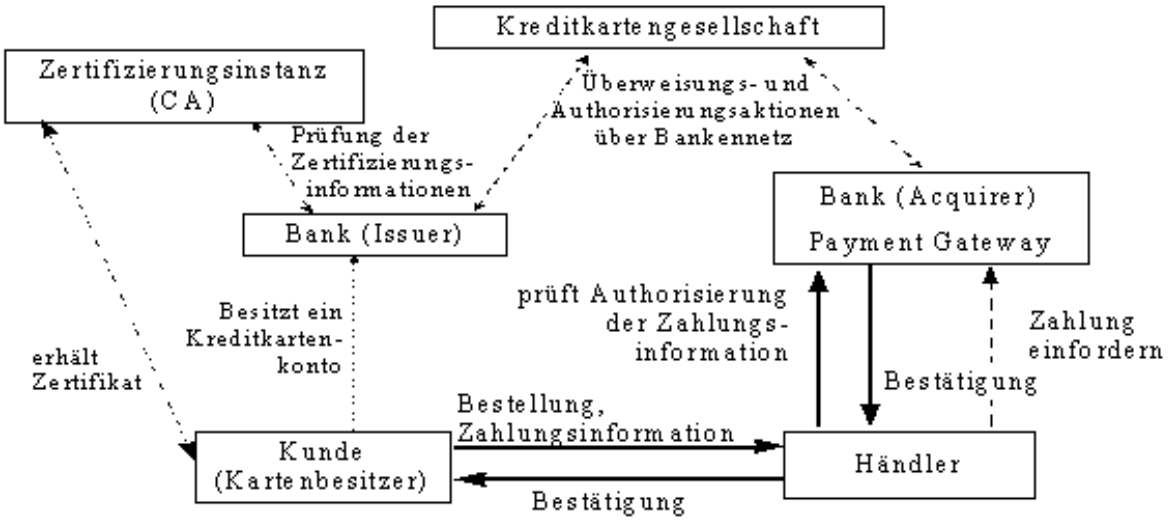
  Zur Autorisierung der Kartenbesitzer, Händler und des Payment Gateway werden Zertifizierungen der öffentlichen Schlüssel vorgenommen.

Zahlungsabwicklung nach dem SET-Protokoll



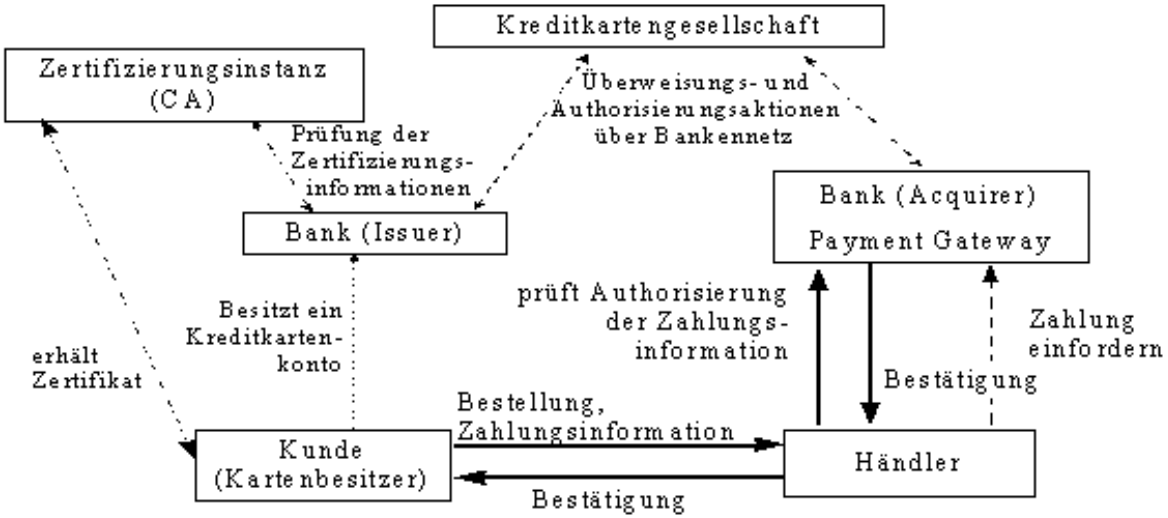
1. Initialisierungsnachricht Kunde an Händler
2. Händler sendet digital signierte Nachricht, die zusätzlich das Verschlüsselungszertifikat mit dem öffentlichen RSA-Schlüssel der Zertifizierungsstelle/Kreditkarteunternehmen/Clearing Stelle enthält.
3. Kunde fertigt signierte Bestellung und signierte Zahlungsanweisung 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

SET-Sicherheitsmechanismen

- Symmetrische Verschlüsselung (DES)
  - für Verschlüsselung der Session Keys
  - Schnelligkeit
- Public-Key-Verfahren mit Einsatz von zwei Public-Key-Schlüssel-Paaren
  - ein Paar für Übergabe der symmetrischen Session Keys (jeweils für Händler und Payment Gateway)
  - ein Paar für Signatur(jeweils für Kunde, Händler und Payment Gateway)

SET-Sicherheitsmechanismen

- Hash-Verfahren (Digest)
- Zertifikate (Problem der gesicherten Schlüsselübergabe)
- Für Kartenzahlung maximale Anonymität
  - Händler: nur Orderinfo
  - Bank: nur Zahlungsinfo

Vor- und Nachteile?

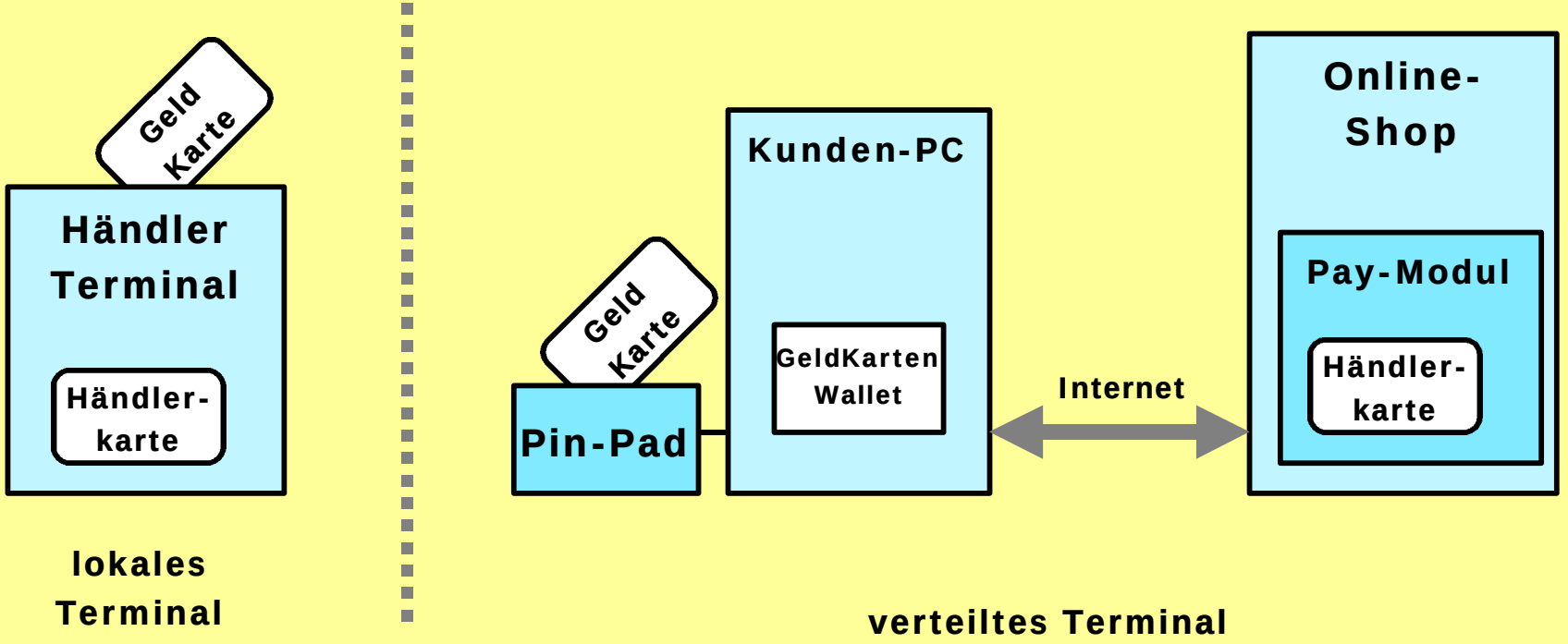
Akzeptanzprobleme

- 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

Bezahlen per Geldkarte im Internet
Beispiel Sparkasse

- Voraussetzung: Kartenlesegerät (seriell oder USB), Geldkarte, Software
- Kunde sucht Waren aus und wählt Zahlungsart „Geldkarte“
- Browser startet Java-Applet, das Rechnungsdaten anzeigt
- Geldkarte wird eingelegt
- Daten werden vor der Übertragung mit einem Kryptogramm versehen (Authentizität)
- Geldkarten-Akzeptanzstelle bucht das Geld ab und schreibt es dem Händler gut
- Geldkarten-Akzeptanzstelle meldet erfolgreiche Gutschrift an Händler, der die Ware auf den Weg bringt

Die GeldKarte im Internet



Net900

- 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
- Summen bis 4,99 DM pro Zeiteinheit/Transaktion möglich
- Geheimnummer für Kontopass wird per „Überweisung“ mitgeteilt

Bezahlen über Handy
paybox

- Vertragspartner wird Handy-Nummer angegeben
- Händler ruft bei Paybox an und gibt Betrag und Mobiltelefonnummer ein
- Paybox ruft Kunden an und läßt sich Bestellung durch Eingabe der paybox-PIN bestätigen
- Betrag wird per Lastschrift eingezogen
- jährliche Grundgebühr für Kunden

Click & buy Firstgate

- Kunde muss sich bei firstgate mit Konto- oder Kreditkartennummer registrieren
- 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

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

Anforderungen an ein Zahlungssystem aus Bankensicht

- Stärkung der Kundenbindung
- Profitabilität